Київський національний торговельно-економічний університет
Кафедра програмної інженерії та кібербезпеки

ВИПУСКНИЙ КВАЛІФІКАЦІЙНИЙ ПРОЕКТ

на тему:

Розробка алгоритмів і методів захисту від інформаційних атак на web-вузли

Студента 4 курсу, 10 групи,
напряму підготовки 6.050103
«Програмна інженерія» _____ Попова Єгора Георгія Сергійовича
підпис студента

Науковий керівник
кандидат технічних наук,
доцент кафедри програмної інженерії та кібербезпеки _____ Рассамакін Володимир Якович
підпис керівника

Гарант освітньої програми
кандидат технічних наук,
доцент кафедри програмної інженерії та кібербезпеки _____ Цензура Микола Олександрович
підпис керівника

КИЇВ - 2019

Київський національний торговельно-економічний університет

Факультет обліку, аудиту та інформаційних систем

Кафедра програмної інженерії та кібербезпеки

Освітній ступінь бакалавр

Напрям підготовки 6.050103 «Програмна інженерія»

Затверджую
Зав. кфедри Криворучко О.В.
_____
"__"_____20__ р.

Завдання
на випускний кваліфікаційний проект студентові

Попова Єгора Георгія Сергійовича
(прізвище, ім'я, по батькові)

1. Тема випускного кваліфікаційного проекту _____
_____

Затверджена наказом ректора від "07" листопада 2018 р. № 185

2. Строк здачі студентом закінченої проекту 10.06.2019
_____

3. Цільова установка та вихідні дані до проекту *Наказ №185 від 07.11.18*
Мета проекту - дослідити існуючі методи захисту веб-вузлів, проаналізувати алгоритми їх дії та розробити алгоритм конфігурації обладнання завдяки якому досягається допустимий рівень безпеки веб-вузлів.
_____

Об'єкт дослідження – захист веб-вузлів і супровідних систем.
_____

Предмет дослідження – методи, способи та алгоритми захисту веб-вузлів.
_____

4. Консультанти проекту із зазначенням розділів, які консультують:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видав	Завдання прийняв

5. Зміст випускного кваліфікаційного проекту (перелік питань за кожним розділом)

ВСТУП_____

РОЗДІЛ 1_____

ТЕОРЕТИЧНІ АСПЕКТИ ПРОБЛЕМ ЗАХИСТУ WEB-ВУЗЛІВ_____

1.1 Причини виникнення загроз_____

1.2 Типи вразливостей web –вузлів_____

1.3 Види загроз для web-вузлів_____

Висновки до розділу 1_____

РОЗДІЛ 2_____

АЛГОРИТМИ І МЕТОДИ ЗАХИСТУ WEB-ВУЗЛІВ_____

2.1 Атаки та методи протидії_____

2.2 Протокол HTTPS_____**Ошибка! Закладка не определена.**

2.3 Удосконалений метод захисту веб-ресурсу_____

Висновки до розділу 2_____

РОЗДІЛ 3_____

РОЗРОБКА АЛГОРИТМІВ І МЕТОДІВ ЗАХИСТУ WEB-ВУЗЛІВ НА_____ ПРИКЛАДІ ТОВ «INTRAFFIC»_____

3.1 Технічна характеристика мережі підприємства ТОВ «Intraffic»_____

3.2 Використовувані протоколи та програмний функціонал _____

3.3 Приклад практичного налаштування мережевого обладнання для_____ забезпечення захисту web-вузла_____

Висновки до розділу 3_____

ВИСНОВКИ ТА ПРОПОЗИЦІЇ_____

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ_____

ДОДАТКИ_____

6. Календарний план виконання проекту

№ пор.	Назва етапів випускного кваліфікаційного проекту	Строк виконання етапів проекту	
		за планом	фактично
1.	*Вибір теми випускного кваліфікаційного проекту*	*21.09.2018*	
2.	*Розробка та затвердження завдання на проект бакалавра (Наказ №185 від 07.11.18)*	*07.11.2018*	
3.	*Вступ та перелік літературних джерел*	*14.12.2018*	
4.	*Розділ 1. Теоретичні аспекти проблем захисту web-вузлів*	*28.01.2019*	
5.	*Розділ 2. Алгоритми і методи захисту web-вузлів*	*01.03.2019*	
6.	*Розділ 3. Розробка алгоритмів і методів захисту web-вузлів на прикладі ТОВ «Intraffic»*	*05.04.2019*	
7.	*Висновки та пропозиції*	*26.04.2019*	
8.	*Підготовка автореферату та презентації доповіді*	*27.05.2019*	
9.	*Зовнішнє рецензування випускного кваліфікаційного проекту*	*05.06.2019*	
10.	*Здача прошитого випускного кваліфікаційного проекту на кафедру*	*10.06.2019*	
11.	*Публічний захист випускної кваліфікаційної роботи*	*18.06.2019 – 21.06.2019*	

7. Дата видачі завдання «07» листопада 2018 р.

8. Науковий керівник випускного кваліфікаційного проекту
Рассамакін В.Я.
(прізвище, ініціали, підпис)

9. Гарант освітньої програми Цензура М.О.
(прізвище, ініціали, підпис)

10. Завдання прийняв до виконання студент Попов Є.Г.С.
(прізвище, ініціали, підпис)

11. Відгук керівника випускного кваліфікаційного проекту

Науковий керівник випускного кваліфікаційного проекту _____
(підпис, дата)

Відмітка про попередній захист _____
(ПІБ, підпис, дата)

12. Висновок про випускний кваліфікаційний проект

Випускний кваліфікаційний проект студента _____Попова Є.Г.С.__
(прізвище, ініціали)

може бути допущена до захисту екзаменаційній комісії.

Гарант освітньої програми _____Цензура М.О._____
(прізвище, ініціали, підпис)

Завідувач кафедри _____Криворучко О.В.____
(підпис, прізвище, ініціали)

«_____»_____20 ___ р.

ЗМІСТ

					КНТЕУ 6.050103 10-26.БР		
					Розробка алгоритмів і методів захисту від інформаційних атак на web-вузли	*Стадія*	*Аркуш*	*Аркуші*
Зм.	*Аркуш*	*№ докум.*	*Підпис*	*Дата*		Зміст	*2*	*35*
.Зав. каф.		Криворучко О.В.						
.Керівник		Рассамакін ВЯ.						
Гарант		Цензура М. О.			*Зміст*	Факультет обліку, аудиту та інформаційних систем,		
Розроб		Попов Е.Г.С.						

ВСТУП

Невелика або велика організація – сьогодні уразливі всі. Dropbox, LinkedIn, Ashley Madison – список відомих жертв можна продовжити, хоча інформація про злам частіше за все навіть не розголошується. Зловмисники завдають величезної шкоди десяткам тисяч працюючих веб-ресурсів, які донедавна вважалися недосяжними для зламу. При цьому, є і позитивний момент: все більше людей починають замислюватися про безпеку власних мереж і веб-вузлів.

Інформація потребує надійного захисту – ця аксіома відома всім. І безсумнівно, більшість користувачів знають, що таке Firewall і троянські віруси і якими засобами можна забезпечити захист мережі. Однак не всі знають, як вони працюють і як оптимально налаштувати систему захисту компанії. Проте саме від цього залежить не тільки збереження даних, а й існування підприємства в цілому.

Проблемам захисту веб-ресурсів присвячена велика кількість досліджень. Так Дж. Скембрейц [1] та Жуков Ю.В. [2] вивчали методи і інструменти атак та захист від них. З інтервалом майже в 10 років автори наочно ілюструють зміни в підходах до захисту веб-ресурсів. Якщо перший стверджував про можливість забезпечити захист від будь-яких атак на ресурси, то другий розглянув конкретні методи та алгоритми дій у випадку атак.

С.М. Сорокін [3] описав метод ідентифікації атак типу «відмова в обслуговуванні», оснований на застосуванні багатошарового персептрону, що дозволило отримати необхідну множину показників.

Розв'язування задачі детектування DDoS-атак на основі розробки спеціальної метрики можна знайти в праці Фаткієва Р.Р. [4] Існуючі методи захисту від DDoS-атак проаналізував J.Sen [5] та запропонував новий метод, який базується на статичному аналізі вхідного трафіка на сервері та надійній системі перевірки гіпотез.

Комбіновані методи захисту веб-ресурсів на основі використання евристичного підходу, в рамках якого виділяється аномальна поведінка споживача, що підвищує ймовірність захисту у порівнянні із сигнатурним аналізом можна побачити в працях Поворознюка А.І. [6]

Цікавим також для вивчення є використання моделей агента загроз для захисту веб-ресурсів від атак, що дає змогу формалізувати пошук вразливостей в інформаційних системах на всіх етапах взаємодії агента загроз із веб-ресурсом. Про це можна дізнатись з досліджень Аласенка А.В. [7].

Актуальність дослідження обумовлена тим, що, незважаючи на високий прогрес в сфері безпеки систем та велику кількість розробок різних методів захисту веб-ресурсів, завжди зловмисники можуть знайти вразливі місця в програмному продукті, а, отже, більшість систем можуть бути піддані впливу збоку зловмисників.

Мета роботи – дослідити існуючі методи захисту веб-вузлів, проаналізувати алгоритми їх дії та розробити алгоритм конфігурації обладнання завдяки якому досягається допустимий рівень безпеки веб-вузлів.

Отже, *об'єктом дослідження* є захист веб-вузлів і супровідних систем.

Предмет дослідження – методи, способи та алгоритми захисту веб-вузлів.

Перелік завдань включає наступне:

-визначити актуальність проблеми захисту веб-вузлів;

-розглянути існуючі методи і алгоритми захисту;

-дослідити систему захисту веб-вузлів на прикладі підприємства ТОВ «Intraffic»;

- розробка переліку загальних методів та алгоритмів для забезпечення захисту веб-вузлів від інформаційних атак;
- за результатом дослідження зробити висновки.

Методи дослідження. Теоретичною основою реалізації визначених в роботі завдань стали дослідження провідних вчених з питань безпеки веб-вузлів. Крім того, включають в себе аналіз, синтез, порівняння, групування та графічне представлення результатів дослідження.

РОЗДІЛ 1

Теоретичні аспекти проблем захисту web-вузлів

1.1 Причини виникнення загроз

Компанії часто ігнорують технічні недоліки на своєму мережевому периметрі, і це рано чи пізно стає джерелом проблем. Здається дивним, але чим більша компанія, тим менше вона може розповісти про те, що і де відбувається в заданий момент часу. До чого готуватися інтернет-компаніям, які працюють на ринках електронної комерції, онлайн-платежів, SaaS/PaaS, Big Data, ЗМІ і персональних комунікацій?

Ще наприкінці 2007 р., були розроблені рекомендації та розглянуті способи компрометації веб-серверів і методи протидії їм. Всі описані тоді методи активно використовуються досі. Використовуючи наведені рекомендації, можна істотно знизити ризик проведення успішної атаки на веб-сервер. Це дозволить уникнути зараження відвідувачів вашого сайту, падіння трафіку з пошукових систем і можливих проблем з індексацією (наприклад, в тих випадках, коли на сторінках сайту хакери розміщують прихований текст з великою кількістю посилань).

Статистика, яка представлена Google, свідчить: за 2016 рік у інтернеті зафіксовано на 32% більше зламів сайтів, ніж роком раніше [1], і в майбутньому прогнозується зростання цього показника. Здавалося б, зі збільшенням кількості і якості засобів захисту загроз сайтам має поменшати. Але статистика – річ уперта, і очевидно, що хакери також успішно вдосконалюють свою майстерність. Розглянемо протокол безпечного з'єднання HTTPS, сертифікати безпеки і види уразливості сайтів.

Цілями зловмисників найчастіше стають сайти банків, мобільних операторів, відомі медіапорталі, урядові установи. Пояснюється це тим, що злом таких сайтів, по-перше, може допомогти заробити чималі гроші, а по-друге, дати доступ до важливої інформації. Піддаються несанкціонованому доступу і ті сайти, аудиторія яких щодня складає кілька тисяч відвідувачів. Але власникам невеликих сайтів не варто помилково відчувати себе в безпеці. Дрібні сайти нерідко використовуються як плацдарм для тренувань для нецільових атак, коли атакують відразу сотні або тисячі ресурсів, обраних за певним критерієм. Є думка, що кожен третій сайт знаходиться під наглядом сторонніх людей, які вивчають його уразливості і в будь-який момент можуть здійснити несанкціоноване втручання.

Отже, головним завданням власника ресурсу є максимальний захист його від всіх можливих загроз, щоб не втратити важливу інформацію і власні гроші.

1.2 Типи вразливостей web-вузлів

Наявність вразливостей пояснюється дуже легко. Людина – не машина, вона може помилятися. Існує навіть спеціальна норма програмування, в якій зазначено, скільки помилок може допустити фахівець при написанні певного числа рядків коду. Крім того, не можна забувати, що велике ПО пише не одна людина, а ціла група. І досить часто помилки виникають при компонуванні модулів, створених різними програмістами. Крім того, наявність вразливостей далеко не завжди визначається якістю написання ПЗ.

Сам термін «уразливість» – це переклад англійського слова vulnerability, що означає недолік в коді сайту або програмному забезпеченні, використовуючи який можна порушити роботу системи.

Часто поява уразливості буває викликана помилками програмування, недоліками при проектуванні сайту або ненадійними паролями.

До основних типів вразливостей відносяться наступні:

- недоліки системи аутентифікації і управління сесією;
- небезпечні прямі посилання на об'єкти;
- небезпечна конфігурація;
- витік чутливих даних;
- відсутність контролю доступу до функціонального рівня;
- використання застарілих компонентів;
- невалідовані редіректи (несанкціоноване перенаправлення);
- клікджекінг (використання невидимих елементів).

Це далеко не повний перелік, до того ж постійно з'являються все нові і нові типи. [2]

Оскільки кожна дія в інтернеті – це обмін даними, то кожен раз, коли користувач відкриває потрібний сайт, комп'ютер надсилає запит серверу і отримує відповідь. Зазвичай обмін йде по протоколу HTTP. Він встановлює правила обміну даними, і саме за його допомогою зміст сайту завантажується на пристрій.

Незважаючи на популярність і зручність використання, дані протоколу абсолютно нічим не захищені, вони передаються у відкритому вигляді. На шляху від комп'ютера користувача до сервера інформація проходить через величезну кількість якихось проміжних пунктів. Якщо хоч один з них взято під контроль сторонніми людьми, які мають злий умисел, дані з легкістю можуть бути перехоплені.

1.3 Види загроз для web-вузлів

Перша причина злому – крадіжка пароля до адміністративної частини сайту. Це може статися через вірус, застарілу версію браузера, з якого введено пароль або навіть через те, що пароль був занадто простим.

Незважаючи на цілком реальну небезпеку хакерського втручання, багато власників сайтів для аутентифікації досі використовують відкритий канал. В результаті цього паролі без проблем перехоплюються шахраями, які мають доступ до мережі, в якій працюють несвідомі користувачі.

Крадіжка паролів – одне з найпоширеніших злочинів в інтернеті. За статистикою, щорічно 15% користувачів стають жертвами шахрайства з кредитними картами або крадіжки їх персональних даних [3].

Інша причина крадіжки клієнтських акаунтів – це саме злом сторонніх сайтів. Отримавши доступ до сайту через вкрадений пароль, хакери неодмінно скористаються і конфіденційною інформацією про клієнтів. Наступним їхнім кроком буде використання цієї інформації з вигодою для себе, наприклад, зняття грошей з банківських карт. Великі сервіси, наприклад, банки, постійно працюють над захистом своїх паролів, тоді як дрібні інтернет-магазини, форуми, торрент-трекери нерідко цим нехтують. Хакери, звичайно, знають про це, і нерідко атакують саме їх.

У серпні 2014 року з'явилася інформація про те, що хакерське угруповання з Росії CyberVor викрала 4,5 млрд облікових записів. Логіни і паролі були вкрадені з 420 000 веб-сайтів. Хакери зламали безліч ресурсів великих компаній, але не залишили поза увагою і дрібні, і навіть особисті сайти. За оцінкою представників американської компанії, HoldSecurity, що займається інформаційною безпекою, в руки до злочинців потрапила найбільша база облікових даних [4].

Найчастіше зломи сайтів відбуваються з вини хостинг-провайдера.

По-перше, це може відбуватися через те, що на сервері встановлено застаріле програмне забезпечення, яке зламати простіше, ніж нове ПЗ.

По-друге, злом відбувається через сусідів по акаунту. Сайти у більшості випадків є сусідами один з одним, а непотрібний або забутий

веб-проект без захисту, легко може бути зламаний. І це потягне за собою і злом всього веб-ресурсу.

По-третє, несанкціонований доступ може відбутися через те, що сайт розміщений у сумнівного провайдера та через відсутність компетенцій або досвіду безпечного адміністрування захисту, сервер буде зламаний через вразливі компоненти і настройки.

Для управління контентом, структурою і дизайном сайту використовуються системи управління сайтом (Content Management System – CMS). Програмування, дизайн та підтримка сайту з використанням таких систем є навіть для людей, що мають дуже туманне уявлення про програмування і взагалі про web-архітектуру. Але, як і всі види ПО, CMS містить уразливості, через які її можна зламати. Особливо ця загроза є актуальною для популярних систем, оскільки їх злом дає можливість зламати відразу десятки тисяч сайтів по всьому світу.

Відповідно до звітів компанії Sucuri, що спеціалізується на web-безпеці, в третьому кварталі 2016 року найбільш зламувати CMS були визнані WordPress – 74%, Joomla – 17% и Magento – 6% від усієї кількості скомпрометованих сайтів [6]. Велика частина зломів сталася від того, що адміністратори вчасно не подбали про встановлення оновлень безпеки системи.

Використовуючи уразливість системи, хакери можуть розміщувати на сайті код, що заражає комп'ютери шкідливими програмами, публікувати контент сумнівного змісту або перенаправляти на інші сайти з таким контентом. Репутація сайту в цьому випадку серйозно страждає.

Злом сайту через модулі та компоненти поза CMS зламати складно навіть хакерам дуже високого рівня. Небезпека криється у всіляких розширеннях - компонентах, плагінах, модулях, що створюються сторонніми розробниками. Наприклад, при установці компонента

коментарів, в якому є «дірка», хакер отримає можливість замість коментаря залити на сайт спеціальний скрипт і зробити злом.

SQL-ін'єкція – це вразливість, що виникає при недостатній перевірці та обробці переданих від користувача даних. Вона дає можливість хакерам модифікувати і навіть виконувати не передбачені кодом програми запити шляхом впровадження шкідливого коду в запит до бази даних. Результатом є отримання доступу до даних, до яких в звичайних умовах доступ заборонений. Використання цієї вразливості дозволяє здійснювати крадіжку даних, їх підміну або знищення і провокувати відмову в обслуговуванні (DDoS).

Є думка, що саме за допомогою SQL-ін'єкцій здійснено витік паролів з сайтів Yahoo, LinkedIn и eHarmony. Звіт компанії Akamai Technologies, Inc. показує, що в 1 кварталі 2016 року збільшення нападів, пов'язаних з SQL-ін'єкціями, зросла на 87% в порівнянні з попереднім періодом. Близько 60% атак припадає на сайти з медіа і розважальним контентом, 30% – на сайти онлайн-послуг і 10% – на урядові сайти [15].

Висновки до розділу 1

Веб-сервери постійно піддаються безлічі самих різноманітних небезпек. Причому найсерйознішу загрозу становлять для них хакери і віруси. Перші можуть отримати доступ до конфіденційної інформації, розміщеної на сервері, зламати сайти і підмінити їх вміст, а також вивести з ладу сервер за допомогою розподіленої атаки (DDoS-атака). Віруси ж, заражаючи веб-сервери, перетворюють їх самих у розсадник інфекції. Використовуючи уразливості, і ті й інші одержують досить легкий доступ до віддаленого web-вузла навіть у тому випадку, якщо останній добре захищений. Практично в будь-якій програмі є вразливості. І чим її вихідний код більше за обсягом, тим більше в ній можна знайти різних «дірок». Саме тому необхідно приділяти значну увагу до інформаційної безпеки будь-якої компанії і вживати міри та заходи для її забезпечення.

РОЗДІЛ 2

Алгоритми і методи захисту web-вузлів

2.1 Атаки та методи протидії

Використовуючи статистичні дані 2017 року, які наведені в таблиці 2.1. [12] Присяжним Д.П. [16] здійснено аналіз і опис атак, а також продемонстровано відсоток веб-ресурсів, до яких вони можуть бути застосовані. Крім того, в тій же роботі запропоновані адекватні методи протидії таким атакам.

Найбільш популярною атакою є «Insufficient transport layer protection» – отримання даних під час передавання. Дана атака може бути виконана для 70% ресурсів. Для виключення можливості проведення таких атак достатньо використовувати протокол HTTPS.

Витік інформації («Information leakage»). Дану атаку можна виконати на 56% ресурсів. Витік інформації з додатків виникає в результаті відмови або неправильної роботи програми, а також у разі порушення її логіки. Для виключення можливості проведення атаки необхідно ретельно тестувати програмну частину ресурсу, проводити перевірку повідомлень на стороні сервера, моніторинг оповіщень про помилки.

Атаку «Cross-site scripting» – міжсайтове використання сценаріїв, можливо виконати на 47% ресурсів. Атака дозволяє передати JavaScript-код на виконання в браузер користувача. Атаки такого роду часто називають HTML-ін'єкціями, адже механізм їх впровадження дуже схожий із SQL- ін'єкціями, але на відміну від останніх, впроваджуваний код виконується в браузері

користувача. Для захисту від цього виду атак необхідно проводити очищення та валідацію вхідних даних.

Таблиця 2.1.

Класифікація видів атак, їхня розповсюдженість і методи протидії

№ з/п	Вид атаки	Вразливість веб-ресурсів, %	Протидія
1	Insufficient transport layer protection	70 %	Використання протоколу HTTPS
2	Information leakage	56 %	Тестування програмної частини ресурсу, перевірка повідомлень на стороні сервера, моніторинг оповіщень про помилки
3	Cross-site scripting	47 %	Очищення та валідація вхідних даних
4	Brute force	29 %	Використання паролів високої складності, налаштування сервера на аналіз вхідних запитів
5	Content spoofing	26 %	Відмовитися від використання фреймів і не передавати в параметрах абсолютні або локальні шляхи до файлів
6	Cross-site request forgery	24 %	Перевірка вхідних даних з форм
7	URL redirector abuse	16 %	Валідація вхідних даних
8	Predictable resource location	15 %	Контроль доступу до файлів сервера

Генерацію великої кількості запитів, або підбір паролів («Brute force») можливо виконати на 29% ресурсів. Для захисту необхідно забезпечити використання паролів високої складності, налаштування сервера на аналіз вхідних запитів.

Атака «Content spoofing» – підміна даних через заміну контенту сторінок можлива для 26%. Використовуючи цю техніку, зловмисник змушує користувача повірити, що сторінка згенерована веб-сервером, а не передана із зовнішнього джерела. Для захисту від даного виду атак потрібно відмовитися від використання фреймів і, найголовніше, ніколи не передавати в параметрах абсолютні або локальні шляхи до файлів.

Вид атак на відвідувача веб-сайтів, який використовує недоліки протоколу HTTP – «Cross-site request forgery». Якщо жертва заходить на сайт, створений зловмисником, від її особи таємно відправляється запит на інший сервер (наприклад, переказ грошей на рахунок зловмисника). Дану атаку можливо виконати на 24% ресурсів. Для захисту необхідно проводити перевірку вхідних даних з форм, наприклад шляхом додавання унікального доданка.

Перенаправлення на інші сайти через підміну початкових посилань («URL redirector abuse») є різновидом помилок перевірки даних і можливе на 16% ресурсів. Вирішенням є валідація вхідних даних.

Ще однією популярною атакою є «Predictable resource location» – знаходження прихованого функціоналу та даних. Доступна на 15% ресурсів і вирішується шляхом контролю доступу до файлів сервера.

З кожним роком статистика атак змінюється: у 2013 році – популярним видом є Витік інформації («Information leakage»), а у 2014 – «Cross-site scripting». Виходячи з наведених даних, можна зробити висновки про те, що для захисту від більшості популярних видів атак достатньо належним чином превіряти вхідні дані. Також рекомендовано використовувати шифрований протокол HTTPS та будувати програмний додаток ресурсу на одному з відомих програмних каркасів (Frame-work) , в якому вбудовані механізми перевірки, шифрування та валідації. Також варто зауважити, що, крім вказаних атак, існують атаки на мережеві служби, наприклад DoS та DDoS. Одним з методів захисту від є використання хмарних технологій і перевірених конфігурацій серверів.

2.2 Протокол HTTPS

Способів захисту від вразливостей існує безліч, в тому числі і від кожного конкретного їх виду. Це, перш за все, використання ліцензійного ПЗ, регулярне

оновлення CMS, відмова від простих паролів і небезпечних браузерів, установка брандмауера. Одним з надійних засобів захисту можна вважати протокол https.

HTTPS – це захисна оболонка для звичайного HTTP, що дозволяє надійно шифрувати передану від користувача до сервера і назад інформацію. Таке шифрування не допускає витоку даних, а значить, захищає сайт від злому.

Перехід на https зовсім не є жорсткою вимогою для всіх без винятку сайтів. Звичайно, якщо сайт працює з платіжними даними клієнтів або будь-який інший персональною інформацією, такий протокол повинен бути встановлений в обов'язковому порядку. У всіх інших випадках переходити чи не переходити на https вирішує тільки власник сайту. Однак неприємності в разі злому загрожують будь-якого сайту – розсилка спаму, автоматичний перехід на сайти сумнівного змісту або навіть повне знищення. До речі, використання https, як показує практика, це серйозний плюс сайту з боку клієнтів і користувачів. Надійність з'єднання викликає з їх боку більше довіри до самої компанії. До того ж сайти з захищеним з'єднанням краще ранжуються пошуковими системами.

Як вже говорилося, протокол http, за яким здійснюється передача даних, практично нічим не захищений, і інформація може стати легкою здобиччю хакерів. Для виключення можливості витоку в 1994 році був створений протокол https, який використовує криптографічний систему SSL / TLS, яка шифрує всі дані, що передаються і дає можливість установки захищеного з'єднання через незахищений канал. При установці з'єднання по протоколу https комп'ютер користувача і сервер спочатку генерують якийсь секретний ключ, а потім вже обмінюються інформацією, при цьому шифруючи її за допомогою даного ключа. Ключ створюється заново при кожному сеансі зв'язку, так що перехопити і підібрати його практично неможливо – він представляє собою число з кількістю знаків більш ста. Для повної надійності використовується ще і цифровий сертифікат для ідентифікації сервера.

Перше, що робить браузер під час активного з'єднання з https, – перевіряє справжність сертифіката. Тільки після його підтвердження починається обмін даними.

Процес переходу сайту на протокол https складається з декількох кроків.

Крок 1. Отримання і настройка сертифіката. Отримати сертифікат можна в центрах сертифікації за окрему плату, але існують і безкоштовні варіанти. Для невеликих фірм вони можуть бути цілком прийнятні, але великі компанії зазвичай віддають переваги платним сертифікатами, які відрізняються розширеною автентифікацією, можливістю включення субдоменів тощо. Крім того, безкоштовні сертифікати іноді збільшують час передачі даних в кілька разів через особливості їх обслуговування. І що дуже важливо, безкоштовний сертифікат не підійде для сайтів з прийомом онлайн-платежів, оскільки невідомо, хто є власником такого сайту. Потім сертифікат потрібно налаштувати. Мета настройки – переадресація всіх запитів з http на https.

Крок 2. Робота з внутрішніми посиланнями. Повні посилання всередині сайту доведеться замінити на відносні за допомогою скриптів. Оскільки після переходу протокол http не замінюється на https автоматично, може виникнути ситуація із завантаженням змішаного контенту. Одночасна дія обох протоколів не забезпечує повноцінного захисту і може привести навіть до того, що сайт зовсім перестане працювати.

Крок 3. Переведення. Після установки сертифікатів сайт стане доступний за двома адресами, з яких залишити потрібно тільки той, який починається з https. Для цього потрібно налаштувати прямий редирект «301» з http на https. Робиться це на сервері, але можна і в htaccess, хоча останній варіант гірше. Після цього навіть http-запити користувачів будуть переадресовуватися на сайт з новим протоколом.

Крок 4. Внесення змін до файл robots.txt. Для того щоб пошукові роботи могли виявити сайт зі зміненим протоколом, потрібно вказати цей протокол в файлі robots.txt.

Крок 5. Включення HTTPS Strict-Transport-Security. Цей процес індивідуальний для кожного сервера, так що універсальних рекомендацій не існує.

І на закінчення необхідно включити Secure Cookies – з цього моменту інформація на ресурсі надійно захищена.

При виборі сертифіката безпеки для сайту (TLS / SSL) можна піти двома шляхами. Якщо у вас невеликий офлайн-бізнес і ви просто хочете донести інформацію про свою компанію до потенційних клієнтів, використовуйте Domain Validation SSL. Цей вид верифікації не дозволить захищати субдомени і вести фінансові операції через сайт. Зате сертифікат робиться швидко, і він почне працювати відразу після того, як ви підтвердите володіння доменом. Це можна зробити декількома способами: через e-mail, через запис в DNS и через хеш-файл.

Для власників сайтів, на яких передбачаються фінансові онлайн-операції необхідна установка сертифікатів типу Business Validation. Такий вид сертифіката надійніше, оскільки підтверджує не тільки володіння доменом, але і зв'язок компанії з сайтом. Для верифікації потрібно відправити в верифікаційний центр пакет документів і прийняти дзвінок на корпоративний номер. Всі сертифікати Business Validation діляться на кілька видів:

Extended Validation SSL – сертифікати з розширеною перевіркою, зазвичай використовуються банками, платіжними системами, великими інтернет-магазинами – тими, хто працює з великими обсягами грошей.

Wildcard SSL – захищає сам сайт і його піддомени. Використовується в тому випадку, якщо передбачається кілька піддоменів з різною регіональною прив'язкою.

SAN SSL – підтримує зовнішні і внутрішні альтернативні доменні імена.

CodeSigning SSL – підтверджує безпеку кодів і програмних продуктів з сайту, стане в нагоді розробникам додатків.

Але який би сертифікат не був вибраний, спочатку необхідно згенерувати запит на його отримання, що містить всю інформацію про господаря домену і відкритий ключ. Запит направляється в центр верифікації. В результаті видається сертифікат і файл з ключем, який ні в якому разі не повинен потрапляти у відкритий доступ[9].

Навіть прагнення до економії не повинно призводити до відмови від забезпечення безпеки даних на сайті. Набагато простіше витратити кошти і час на її забезпечення, ніж після злому приводити сайт в порядок і боротися з негативною репутацією, яку спровокував цей злом. А якщо сайт має відношення до онлайн-торгівлі, то його безпека повинна бути основним завданням власника.

2.3 Удосконалений метод захисту веб-ресурсу

Як свідчать статистичні дані [12] та запропоновані методи, які орієнтовані на захист від конкретного типу атаки, зловмисна дія на веб-ресурс відбувається, як правило, із використанням відразу декількох різних типів атак. Тому задачею системи менеджменту інформаційної безпеки є розробка ефективної стратегії протидії атакам зловмисників за умови, що вони використовують комбіновані типи атак. Рівень ефективності при цьому визначається замовником веб-ресурсу і задається він специфікою ведення бізнесу підприємством (чи діяльністю організації), параметрам, що характеризують специфіку інформації та баз даних, які належать до конфіденційних і рядом інших параметрів і характеристик.

Розробка такої стратегії захисту веб-ресурсу є нетривіальною задачею. Наведемо удосконалений метод захисту веб-ресурсу, який відрізняється від

аналогів одночасним здійсненням системного, евристичного та статистичного аналізу вразливостей веб-ресурсу, що дозволяє здійснити якісний захист від зловмисників. Які використовують декілька типів атак.

Присяжний Д.П. у своїй роботі «Удосконалення захисту веб-ресурсів від атак на основі комбінованого евристично-статистичного підходу» пропонує метод захисту веб-ресурсу у такій формі [16]:

1 етап. Формуємо множину М характеристик веб-ресурсу, яка включає в себе бази даних, які потрібно захистити від атак, а також характеристики, які описують існуючі системи захисту. Крім того, до цієї множини відносяться характеристики, які визначають специфічні методи та технології взаємодії із користувачами веб-ресурсу.

2 етап. Множину М характеристик веб-ресурсу передаємо до Системи менеджменту інформаційної безпеки для веб-ресурсу, який здійснює аналіз існуючих вразливостей і розробляє систему заходів для захисту веб-ресурсу. Ця діяльність, що описується в етапах 3-5, здійснюється в паралельному режимі за достатніх ресурсів чи у послідовному режимі, коли наявних ресурсів замало.

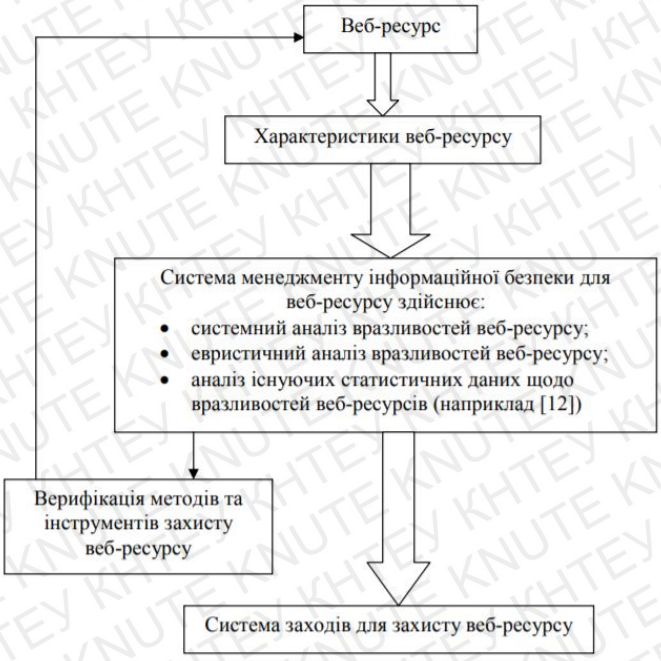


Рис.2.1 Структура методу формування системи захисту веб-ресурсу

3 етап. Здійснюємо системний аналіз вразливостей веб-ресурсу до атак. До задач цього аналізу включаємо: знаходження множини Т цілей для атак і множини цілей ТР для захисту веб-ресурсу; аналіз обмежень як технічного, так і програмного та інформаційного характеру; аналіз простору альтернатив А (як для здійснення а так на веб-ресурс, так і для його захисту); вибір критеріїв ефективності С захисту веб-ресурсу; синтез адекватної моделі для системи захисту веб-ресурсу; розробку рекомендації R для впровадження.

4 етап. Здійснюємо евристичний аналіз вразливостей веб-ресурсу. Цей етап є необхідним, через те, що робота веб-ресурсу із користувачами є слабоформалізованою, і тому для неї часто неможливо знайти адекватні моделі та методи формального опису. До того ж на цьому етапі також здійснюється аналіз поведінки можливих зловмисників і прогнозування типів атак, які вони можуть використати.

5 етап. Здійснюється аналіз для статистичних даних щодо поточного стану вразливостей конкретного веб-ресурсу із використанням існуючих статистичних баз даних, які носять загальний характер. Як правило, виділяється перелік найбільш уживаних типів атак на веб-ресурс і використовуються такі методи протидії, які можна застосувати для декількох типів атак. Наприклад, як видно із таблиці, для атак «Cross-site request forgery» та «URL redirector abuse» методи протидії локалізуються на вхідних даних.

6 етап. За результатами здійсненого аналізу у пп.3-5 Система менеджменту інформаційної безпеки для веб-ресурсу формує систему заходів (узгоджених між собою методів та інструментів) для захисту заданого веб-ресурсу.

7 етап. Здійснюється верифікація запропонованої системи захисту веб-ресурсу від атак. Для цього можуть бути використані існуючі та розроблені тестові та комп'ютерні програми, задіяні спеціалісти з перевірки захищеності від атак тощо. У разі виявлення недостатнього рівня захисту веб-ресурсу, що

виражається у невідповідності характеристик захисту множині критеріїв С, розробленої на етапі 2, етапи 1-6 повторюються.

8 етап. У випадку, коли досягнуто заданого рівня захисту, система захисту даного веб-ресурсу фіксується та впроваджується.

У разі потреби, запропонований метод повторюється із потрібною періодичністю.

Описане удосконалення захисту веб-ресурсів від атак, який на відміну від існуючих, базується на одночасному здійсненні системного, евристичного та статистичного аналізів вразливостей ресурсу, що дозволяє здійснити якісний захист веб-ресурсу від атак. Запропонована система захисту веб-ресурсу використовує віднесення ресурсу до вразливості стосовно певного виду атак.

Крім того, запобіжним методом є перевірка сайту на вразливість. Для цього рекомендується провести тестування на проникнення. Зазвичай воно дозволяє виявити помилки, які зловмисники можуть використовувати для злому вашого сайту. Якісне тестування є багатоступеневим. Його головними етапами є:

- розвідка, в ході якої збирається вся інформація про ваш сервер;
- сканування – безпосередня перевірка на уразливості, виходячи із зібраної інформації;
- експлуатація - необхідна для демонстрації реальної небезпеки вразливостей;
- виправлення - усунення всіх знайдених на сайті проблем.

Безпека і репутація веб-ресурсу – речі нерозривно пов'язані. І справа тут не тільки в тому, що репутацію порталу можна втратити після його злому. Велика ймовірність того, що саме довіру до веб-ресурсу не вдасться отримати з боку відповідальних відвідувачів, які зазвичай складають платоспроможну частину потенційних клієнтів і стежать за наявністю «закритого замочка». Не

кажучи вже про те, що без використання засобів безпеки можуть погіршитися позиції в пошуковій видачі в порівнянні з конкурентами.

Висновки до розділу 2

Виходячи з наведених у розділі даних, можна зробити висновки про те, що для захисту від більшості популярних видів атак достатньо належним чином перевіряти вхідні дані. Рекомендовано використовувати шифрований протокол HTTPS та будувати програмний додаток ресурсу на одному з відомих фреймворків, в якому є вбудовані механізми перевірки, шифрування та валідації. Також варто зауважити, що, крім вказаних атак, існують атаки на мережеві служби, наприклад DoS та DDoS. Саме від атак на мережевому рівні найскладніше захиститися, оскільки вони використовують вразливості фундаментальних протоколів роботи мережі, і внести зміни до них – іноді буває неможливо. Основна частина мережевої безпеки лежить у зоні відповідальності інтернет-провайдерів, які надають доступ до інтернету через власне обладнання. Якщо обладнання провайдера не налаштоване належним чином – це повністю нівелює міри безпеки, прийняті з боку веб-вузлів.

РОЗДІЛ 3

Розробка алгоритмів і методів захисту web-вузлів на прикладі ТОВ «Intraffic»

3.1 Технічна характеристика мережі підприємства ТОВ «Intraffic»

ТОВ «Intraffic» – це інтернет-оператор з власним покриттям, пулом IP-адрес та кількістю абонентів – понад 6000. Основною спеціалізацією є надання доступу до інтернету по комутованим лініям надійного зв'язку.

Згідно з «Ієрархічною моделлю мережі»[21] мережа ТОВ «Intraffic» являє собою: «Ядро мережі», «Рівень розподілення» та «Рівень доступу».

«Ядро» - це комплекс мережевих пристроїв (маршрутизаторів і комутаторів), що забезпечують резервування каналів і високошвидкісну передачу даних між різними сегментами рівня розподілу. На цьому рівні компанією використовується декілька комутаторів з функціоналом третього рівня «Dlink DGS-3620» та маршрутизатор Cisco 7604.

На «Рівні розподілення» вирішуються завдання агрегації широкомовних доменів і доменів маршрутизації, фільтрації і налаштування QoS, агрегації великих дротових мереж в комунікаційній шафі, забезпечення високого рівня доступності ядра для кінцевих користувачів. Маршрутизатор, що використовуються на рівні розподілу також можуть брати на себе функції забезпечення доступу в Інтернет для підрозділів компанії. На цьому рівні використовуються комутатори DGS-3100, DGS-3200 та DGS-3400.

«Рівень доступу» служить для підключення робочих станцій і серверів до мережі компанії. У більшості випадків рівень доступу представлений в

мережі комутаторами другого рівня. Як правило, для організації цього самого простого рівня ієрархічної моделі встановлюються найбільш оптимальні за ціною пристрою, які не потребують складної конфігурації. Основне завдання таких пристроїв – надання доступу робочих станцій і серверів до наступного рівня (розподілу) ієрархії. Найчастіше нашою компанією на цьому рівні задіяні комутатори Dlink DES-3500 та DES-3200.

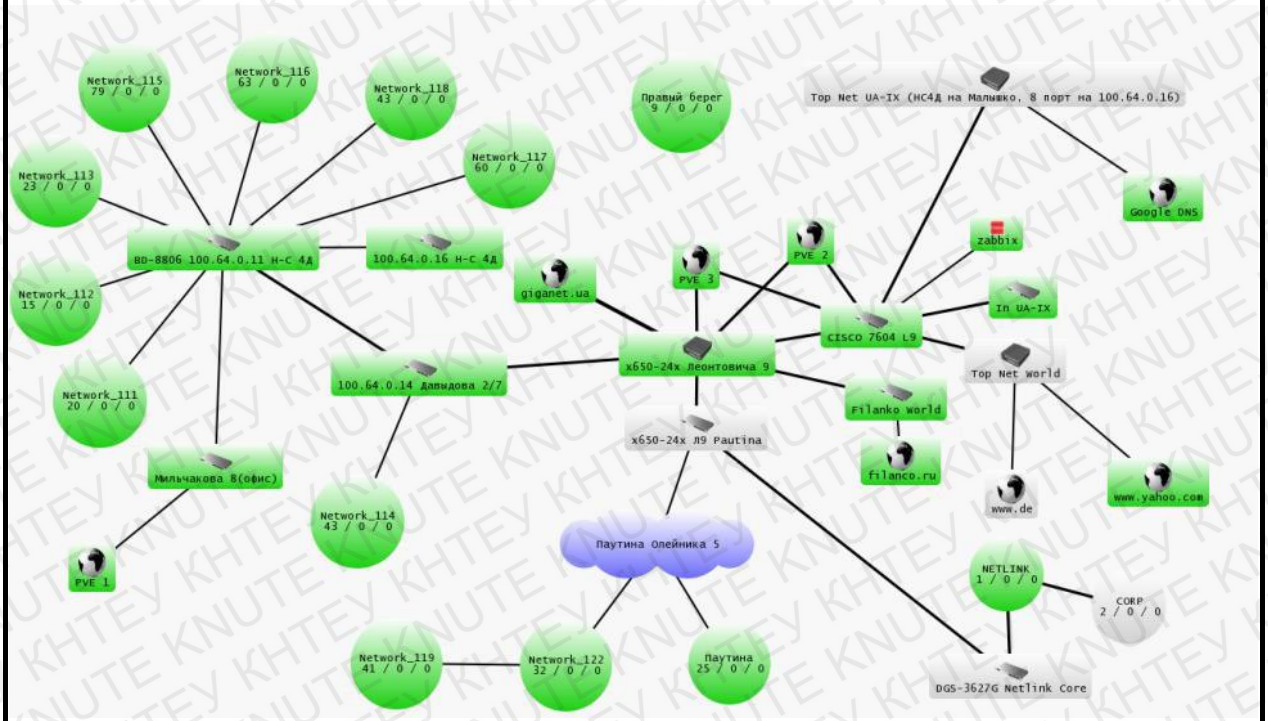


Рис. 3.1. Графічна модель «Ядра м ережі» ТОВ «Intraffic»

На рисунку 3.1. представлена графічна модель «Ядра мережі» ТОВ «Intraffic», на якій зображено центральний маршрутизатор Cisco 7604, комутатори з функціоналом третього рівня Dlink DGS-3620, декілька супроводжуючих сервісів та наявні підмережі.

3.2 Використовувані протоколи та програмний функціонал підприємства ТОВ «Intraffic»

Підприємство ТОВ «Intraffic» у своїй роботі використовує наступний програмний функціонал та протоколи:

Telnet – мережевий протокол для реалізації текстового інтерфейсу по мережі. Назву «telnet» мають також деякі утиліти, що реалізують клієнтську частину протоколу.

SSH – мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів). Схожий за функціональністю з протоколом Telnet і rlogin, проте шифрує весь трафік, в тому числі і паролі, що передаються.

Blackhole – ця технологія (також відома як Null-route) застосовується в боротьбі з DDoS-атаками, які спрямовані на вичерпання ємності каналу зв'язку. При включеному Blackhole-маршруті весь трафік на атакований IP або префікс блокується у оператора-аплінка, звільняючи канал від сміттєвого трафіку.

LISG – система, яка займається контролем сесій користувачів та веде статистику.

ZABBIX – вільна система моніторингу служб і станів комп'ютерної мережі. Здатна до автоматичного виявлення загроз и проблемних ситуацій.

Graylog – агрегатор логів з мережевого обладнання, з функцією пошуку по заданим ключовим характеристикам.

3.3 Приклад практичного налаштування мережевого обладнання для забезпечення захисту web-вузла

Основні розділи алгоритму налаштування програмованого комутатора Dlink серії 3500 підприємства ТОВ «Intraffic», які забезпечують припустимий рівень захисту виглядають таким чином:

Base

enable password encryption
enable command logging
enable clipaging
disable telnet
disable web
enable ssh

У цьому розділі вмикається шифрування паролю, ведення логу

введених команд та доступ через зашифрований протокол зв'язку. Вимикається можливість з'єднатися з комутатором через незашифрований канал та доступ через веб-інтерфейс браузера.

Filter_dhcp

config filter dhcp_server ports {{{CUSTOMER_PORTS}}} state enable
config filter dhcp_server ports {{{DOWNLINK_PORTS}}} state enable
config filter dhcp_server trap enable
config filter dhcp_server log enable

У даній секції вмикається фільтрування DHCP-пакетів на абонентських та даунлінкових портах. Також вмикається ведення логу щодо проходження DHCP-пакетів крізь порти комутатора.

Sntp

config time_zone operator + hour 2 min 0
config sntp primary 192.168.{{{SUBNET_ID}}}.250 secondary 94.232.215.28 poll-interval 3600
config dst repeating s_week last s_day sun s_mth 3 s_time 03:00 e_week last e_day sun e_mth 10 e_time 04:00 offset 60
enab sntp

У цьому розділі задаються налаштування для роботи спрощеного мережевого протоколу часу, а також вказується час синхронізації його із сервером.

safeguard_engine

config safeguard_engine state enable utilization rising 90 falling 70
config safeguard_engine trap_log enable

Тут вказано у відсотках межу завантаженості процесора, після якого комутатор переходить у "захищений режим".

loopdetect

config loopdetect recover_timer 60
config loopdetect interval 2
config loopdetect ports {{{CUSTOMER_PORTS}}} state enabled
config loopdetect ports {{{DOWNLINK_PORTS}}} state enabled
enable loopdetect

У цьому розділі вказано порти, на яких налаштовується захист від мережевих "петель", а також час, після якого виконується повторна перевірка на наявність "петлі".

authen_radius

create authen server_host 94.232.215.29 protocol radius port 1812 key "1qazZAQ!" timeout 2 retransmit 2

create authen server_host 100.64.0.10 protocol radius port 1812 key "1qazZAQ!" timeout 2 retransmit 2
config authen server_group radius delete server_host 94.232.215.29 protocol radius
config authen server_group radius delete server_host 100.64.0.10 protocol radius
config authen server_group radius add server_host 94.232.215.29 protocol radius
config authen server_group radius add server_host 100.64.0.10 protocol radius
config authen_login default method local
create authen_login method_list_name rad_ext
config authen_login method_list_name rad_ext method radius local
config authen_enable default method local_enable
create authen_enable method_list_name rad_ext_ena
config authen_enable method_list_name rad_ext_ena method radius local
config authen application all login method_list_name rad_ext
config authen application all enable method_list_name rad_ext_ena
config authen parameter response_timeout 0
config authen parameter attempt 3
enable authen_policy

В даному розділі вказується сервер для підключення за протоколом RADIUS, а також виконується налаштування методів та політик аутентифікації.

syslog

enable syslog
create syslog host 2 ipaddress 100.64.0.115 udp_port 514 severity all facility local6 state enable
create syslog host 3 ipaddress 94.232.215.28 udp_port 514 severity all facility local6 state enable
create syslog host 4 ipaddress 192.168.{{{SUBNET_ID}}}.254 udp_port 514 severity all facility local6 state enable

Тут вказуються адреси серверів, на яку буде вивантажуватись лог комутатора, що забезпечить захист даних і доступ до них під час діагностики.

dhcp_relay

enable dhcp_relay
config dhcp_relay option_82 state enable
config dhcp_relay option_82 check enable
config dhcp_relay option_82 policy keep
config dhcp_relay ports {{{UPLINK_PORT}}} state disable
config dhcp_relay ports {{{DOWNLINK_PORTS}}} state disable
config dhcp_relay add vlanid {{{CUSTOMER_VLAN}}} 100.64.0.10
config dhcp_relay add vlanid {{{CUSTOMER_VLAN}}} 100.64.0.20

Тут виконується налаштування функціоналу, який забезпечує передачу DHCP-пакетів від сервера, який знаходиться в іншій підмережі.

address_binding

config address_binding ip_mac ports {{{CUSTOMER_PORTS}}} ip_inspection enable

config address_binding ip_mac ports {{{CUSTOMER_PORTS}}} arp_inspection strict
config address_binding ip_mac ports {{{CUSTOMER_PORTS}}} allow_zeroip enable
config address_binding ip_mac ports {{{CUSTOMER_PORTS}}} protocol ipv4
enable address_binding dhcp_snoop
enable address_binding trap_log

В даному розділі виконується налаштування прив'язки IP-адреси до MAC-адреси і до порту комутатора, а також вказується рівень захисту і протокол.

traffic_segmentation

config traffic_segmentation {{{customer_ports}}} forward_list {{{uplink_port}}}
config traffic_segmentation {{{downlink_ports}}} forward_list {{{uplink_port}}}

Тут налаштовується сегментація трафіку, вказуються порти, пакети з яких можуть йти тільки крізь конкретні інші порти.

lldp

enable lldp
config lldp ports all admin_status tx_and_rx
config lldp ports all basic_tlvs all enable

Тут вмикається робота протоколу LLDP, який дозволяє збирати дані про оточуюче мережеве обладнання, на якому теж увімкнений даний протокол.

vlan

config vlan vlanid 1 delete {{{customer_ports}}},{{{uplink_port}}}
config vlan vlanid 1 delete {{{downlink_ports}}}
create vlan {{{customer_vlan}}} tag {{{customer_vlan}}}
create vlan {{{management_vlan}}} tag {{{management_vlan}}}
config vlan vlanid {{{customer_vlan}}} add untagged {{{customer_ports}}}
config vlan vlanid {{{customer_vlan}}} add tagged {{{uplink_port}}}
config vlan vlanid {{{management_vlan}}} add tagged {{{uplink_port}}}
config vlan vlanid {{{customer_vlan}}} add tagged {{{downlink_ports}}}
config vlan vlanid {{{management_vlan}}} add tagged {{{downlink_ports}}}

В даному розділі виконується налаштування VLAN. Для абонентів і управління – використовується два різні VLAN. Це дозволяє розділити абонентів від мережі управління, і зменшує загальну кількість флуду у мережі.

igmp_snooping

enable igmp_snooping
config igmp_snooping all state enable
config multicast port all filter_unregistered_groups

Тут вмикається можливість відстежувати мультикастовий трафік між

абонентами и мережею.

snmp

enable snmp
config snmp system_contact (044)200-44-00
config snmp system_name {{{subnet_id}}}.{{{sw_last_octet}}}.intraffic

У цьому розділі е можливість вказати контакти власника системи. Іноді це дозволяє повернути загублений комутатор.

snmp_trap

enable snmp traps
enable snmp linkchange_traps
config snmp linkchange_traps ports all enable
enable snmp authenticate traps
config snmp warmstart_traps enable
config snmp coldstart_traps enable
config configuration trap save enable
config configuration trap upload enable
config configuration trap download enable
config loopdetect trap both
create snmp host 100.64.0.24 v2c public
create snmp host 94.232.215.18 v2c public

Тут налаштовується спрощений протокол керування мережевим обладнанням. Вказуються події, у разі спрацювання яких необхідно відіслати на сервер відповідне сповіщення, а також зробити запис до логу.

ipif/iproute

config ipif system ipaddress 192.168.{{{subnet_id}}}.{{{sw_last_octet}}}/24
config ipif system vlan {{{management_vlan}}}
create iproute default 192.168.{{{subnet id}}}.1

Тут створюється статичний маршрут до мережі з якої виконуються управляння мережевим обладнанням.

Висновки до розділу 3

Компанія ТОВ «Intraffic» у своїй практичній діяльності приділяє більш ніж достатню увагу ефективній політиці безпеки. Для цього періодично виконується оновлення програмного забезпечення на мережевому обладнанні та усіх периферійних системах. Крім того, вчасно виконується заміна застарілого обладнання.

Для покращення заходів безпеки в ході дослідження, крім вказаного раніше, автором запропоновано наступне:

- на корпоративному рівні відмовитись від використання незашифрованого протоколу доступу до мережевого обладнання Telnet;
- за замовчуванням заборонити або відключити проходження трафіку через усі порти TCP та UDP , які не мають поширеного використання і можуть бути пристосовані зловмисниками для зловживань;
- використовувати функціонал traffic_segmentation на всіх абонентських портах, для запобігання можливого впливу зловживання одного абонента на іншого, в межах одного комутатора;
- вмикати dhcp_filter на шляху від абонентів до аплінка для нівеляції можливого впливу флуду, створеного при неправильному підключенні маршрутизатора з боку користувача;

Таким чином, виконуючи, серед інших, запропоновані методи – можна підвищити рівень стабільності роботи мережі, а отже і конкретного веб-вузла.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

В ході розвитку інформаційних технологій і поширення мережі інтернет значно знизилась безпека особистих даних. З кожним роком збільшується кількість кібератак спрямованих, як на великі підприємства, так і на простих користувачів мережі. Ці події значно знижують рівень конфіденційності даних і призводять до великих матеріальних і моральних втрат.

На сьогоднішній час існує чимало дієвих методів здійснення кібератак, які дозволяють спрямовувати злочини не тільки проти незахищених користувачів, а навіть проти цілої держави, цим самим завдаючи їй великих збитків.

При дослідженні алгоритмів захисту від здійснення комп'ютерних злочинів, було виявлено, що вони хоч і дозволяють в деяких випадках запобігти втраті даних, проте вони не дають гарантії захисту від кібератак.

Отже, можна зробити висновок, що кібератаки є досить потужним і поширеним видом злочину в світі і не існує стовідсоткового захисту від нього.

Для практичної реалізації системи захисту веб-вузлів від інформаційних атак обрано підприємство ТОВ «Intraffic».

Компанія ТОВ «Intraffic» у своїй діяльності приділяє достатню увагу створенню ефективної політиці безпеки. Для цього періодично виконується комплекс мір та заходів для підтримки високого рівня безпеки та запобіганню можливих загроз.

Результатом реалізації випускного кваліфікаційного проекту стало впровадження ряду пропозицій, апробація їх на практиці та подальше застосування у роботі підприємства, що має документальне підтвердження.

Список використаних джерел

1. Скембрейц Дж. Безопасность Web-приложений – готовые решения/ Дж. Скембрейц, М. Шема. – М.: Издательский дом «Вильямс», 2003. – 384 с.
2. Жуков Ю.В. Основи веб-хакинга: нападение и защита/ Ю.В. Жуков. – СПб.: Питер, 2011. – 176 с.
3. Сорокін С.Н. Метод обнаружения атак типа «отказ в обслуживании» на WEB-приложения / С.Н. Сорокін// Прикладная дискретная математика. – 2014. – № 1(23). – с. 55–64.
4. Фатикеева Р.Р. Разработка метрик для обнаружения атак на основе анализа сетевого трафика / Р.Р. Фатикеева// Вестник Бурятского государственного университета. – 2013. – Vol. 9. – с. 81-86.
5. Sen J. A Robust Mechanism for Defending Distributed Denial OF Service Attacks on Web Servers / J. Sen // International Journal of Network Security & Its Applications (IJNSA). – 2011, March. – Vol. 3, N 2. – P. 162–179.
6. Поворознюк А.И. Совершенствование защиты Web-приложений от вторжений на основе эвристического похода / А.И. Поворознюк, М.Н. Шкарупа: сб. науч. тр. «Вестник НТУ «ХПИ». Інформатика і моделювання. – 2007. – Вип. 19. – с. 145-154.
7. Аласенко А.В. Разработа и системный анализ математической модели угроз, модели нарушителя, процедур защиты WEB-приложений на всех этапах функционирования / А.В. Аласенко, П.И. Дзьобан // Научний журнал КубГАУ. – 2014. – № 101(07). – с. 1-11.
8. Bhavani A.B. Cross-site Scripting Attacks on Android WebView / A.B. Bhavani // International Journal of Computer Science and Network.

					КНТЕУ 6.050103 10-26.БР			
					Розробка алгоритмів і методів захисту від інформаційних атак на web-вузли	*Стадія*	*Аркуш*	*Аркушів*
Зм.	*Аркуш*	*№ докум.*	*Підпис*	*Дата*		СД	*32*	*35*
.Зав. каф.		Криворучко О.В.						
.Керівник		Рассамакін В.Я.						
Гарант		Цензура М. О.			*Список використаних джерел*	Факультет обліку, аудиту та інформаційних систем, 4 курс, 10 група		
Розроб		Попов Є.Г.С.						

– 2013. – Vol. 2, Issue 2. – 5ı. – Режим доступу: http://ijcsn.org/IJCSN-2013/2-2/IJCSN-2013-2-2-03.pdf.

9. Cuff P. Distributed channel synthesis / P. Cuff // IEEE. Trans. Inf. Theory. – 2013. – Vol. 59(11). – P. 7071-7096.

10. Schieler C. Rate-distortion theory forsecrecy systems / C. Schieler, P. Cuff // IEEE Trans. on Inf. Theory. – 2014. – Vol. 66(12). – P.7584-7605.

11. Sahin C.S. General Framework for Evaluating Password Complexity and Strength / C.S. Sahin, R. Lychev, N. Wagner. – 11 ı. – Режим доступу: http://arxiv.org/abs/1512.05814

12. Website Security Statistics Report: 2015. – WhiteHat Security, 2015. – 30 p. – Режим доступу: https://info.whitehatsec.com/Website-Stats-Report-2015.html

13. Handbook on Ontologies / eds. S. Staab and R. Studer. – International Handbooks on Information Systems. – Berlin: Springer, 2009. – 832 p.

14. Новиков Д.А. Теория управления организационными системами / Д.А. Новиков. – М.: Физматлит, 2007. – 584 с.

15. Протокол HTTPS и уязвимости сайта: безопасные связи – Режим доступу: https://www.kp.ru/guide/bezopasnost-saita.html

16. Присяжний Д.П. «Удосконалення захисту веб-ресурсів від атак на основі комбінованого евристично-статистичного підходу» – Режим доступу: http://www.ipri.kiev.ua/fileadmin/XXXX/2016/1/1-7.pdf

18. HTTPS on Stack Overflow: The End of a Long Road. – Режим доступу: https://nickcraver.com/blog/2017/05/22/https-on-stackoverflow/?utm_source=telegram.me&utm_medium=social&utm_campaign = vchera-stack-overflow-vklyuchili-https-po-d#performance-http2.

19. Дослідження вразливостей Web-сайтів та методів їх усунення – Режим доступу: http://phone.kpi.ua/wp-content/uploads/2014/06/4.pdf

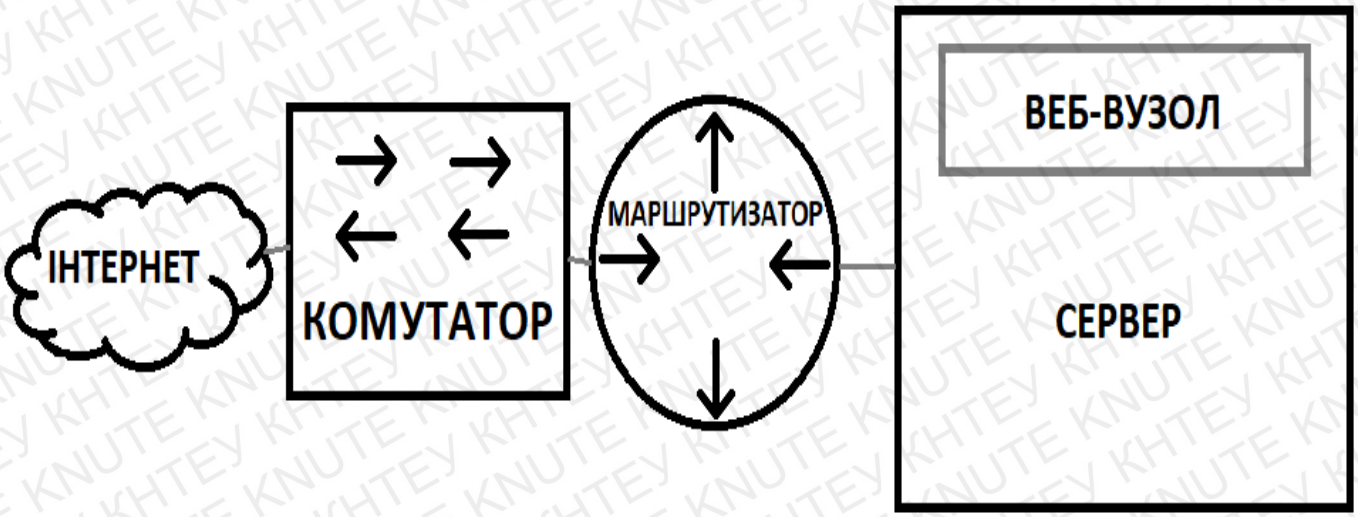
20. http://www.iksmedia.ru/news/5393459-Vzlom-sajtov-na-tret-bolshe-chem.html

21. https://en.wikipedia.org/wiki/Hierarchical_internetworking_model
22.https://joomlaportal.ru/news/security/2844-top-3-samykh-vzlamyvaemykh-cms-po-versii-sucuri
23. https://elibrary.ru/item.asp?id=27538069
24. Center for Internet Security – http://www.cisecurity.org;
25. Microsoft – www.microsoft.com/technet/itsolutions/security/tools/tools.asp;
25. Apache – http://httpd.apache.org/docs/misc/security_tips.html ;
26. Sun – http://www.sun.com/security/blueprints/.

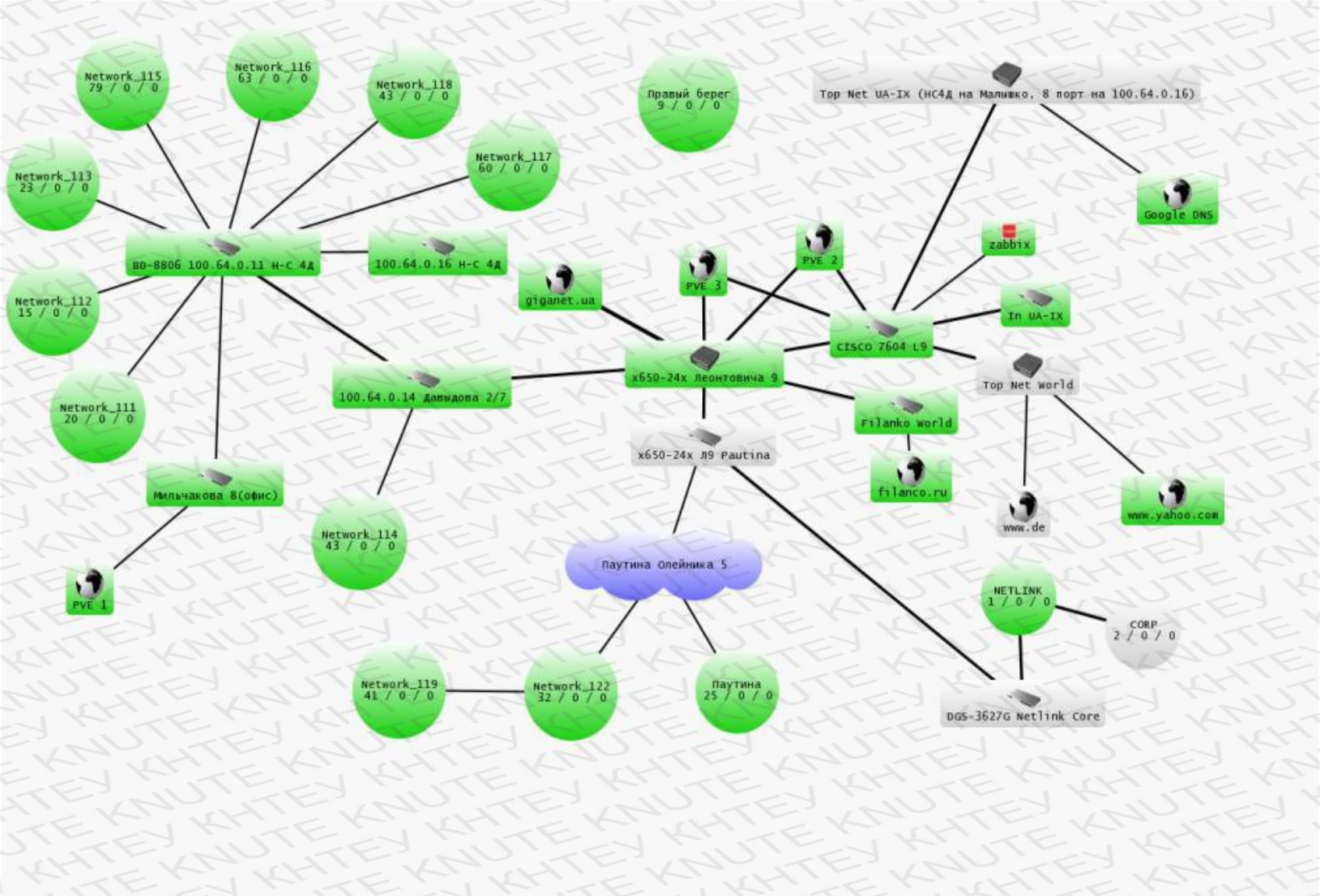
ДОДАТКИ

Додаток А

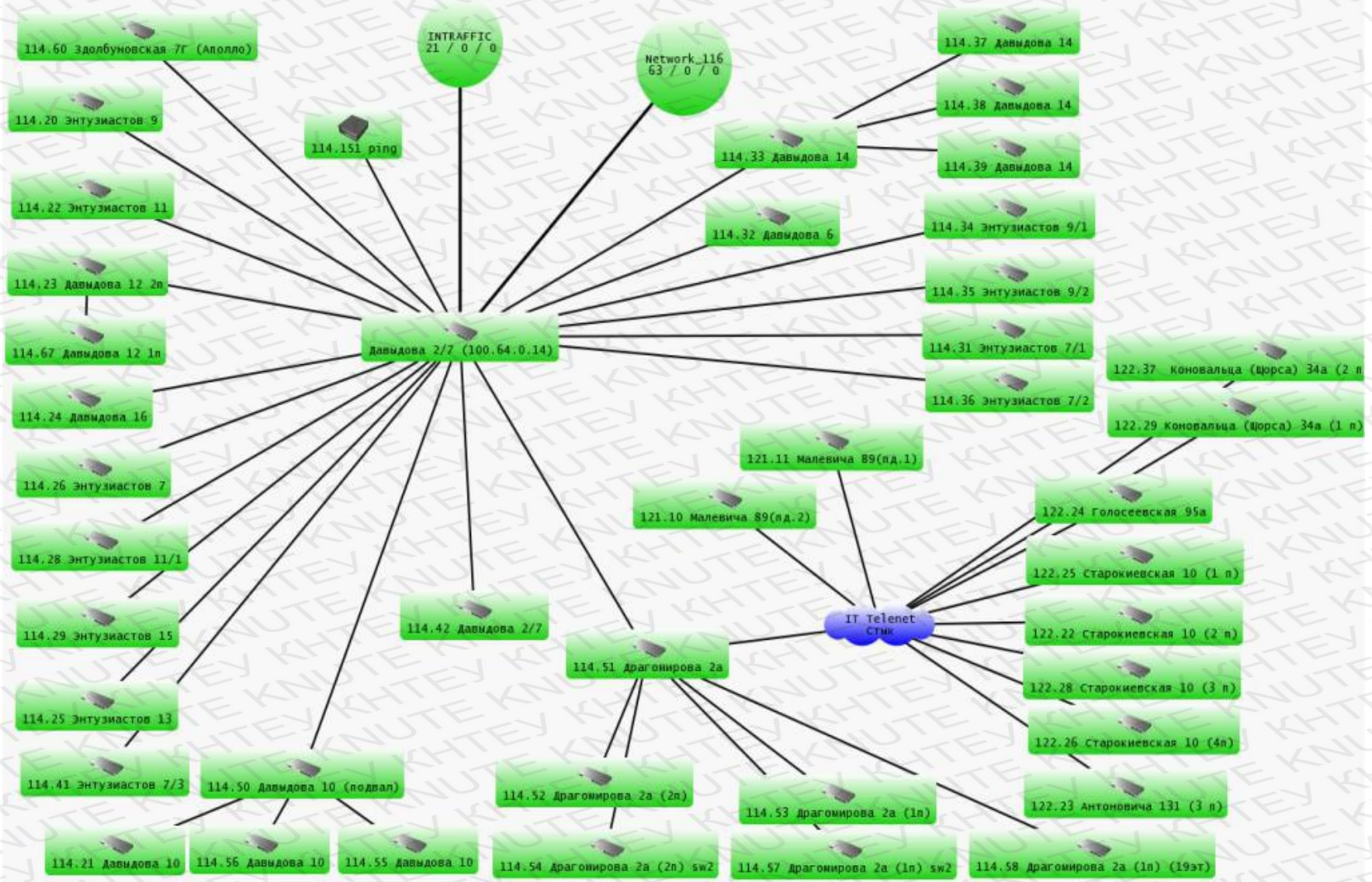
Схематичне зображення ділянки мережі від веб-вузла – до зони відповідальності провайдера



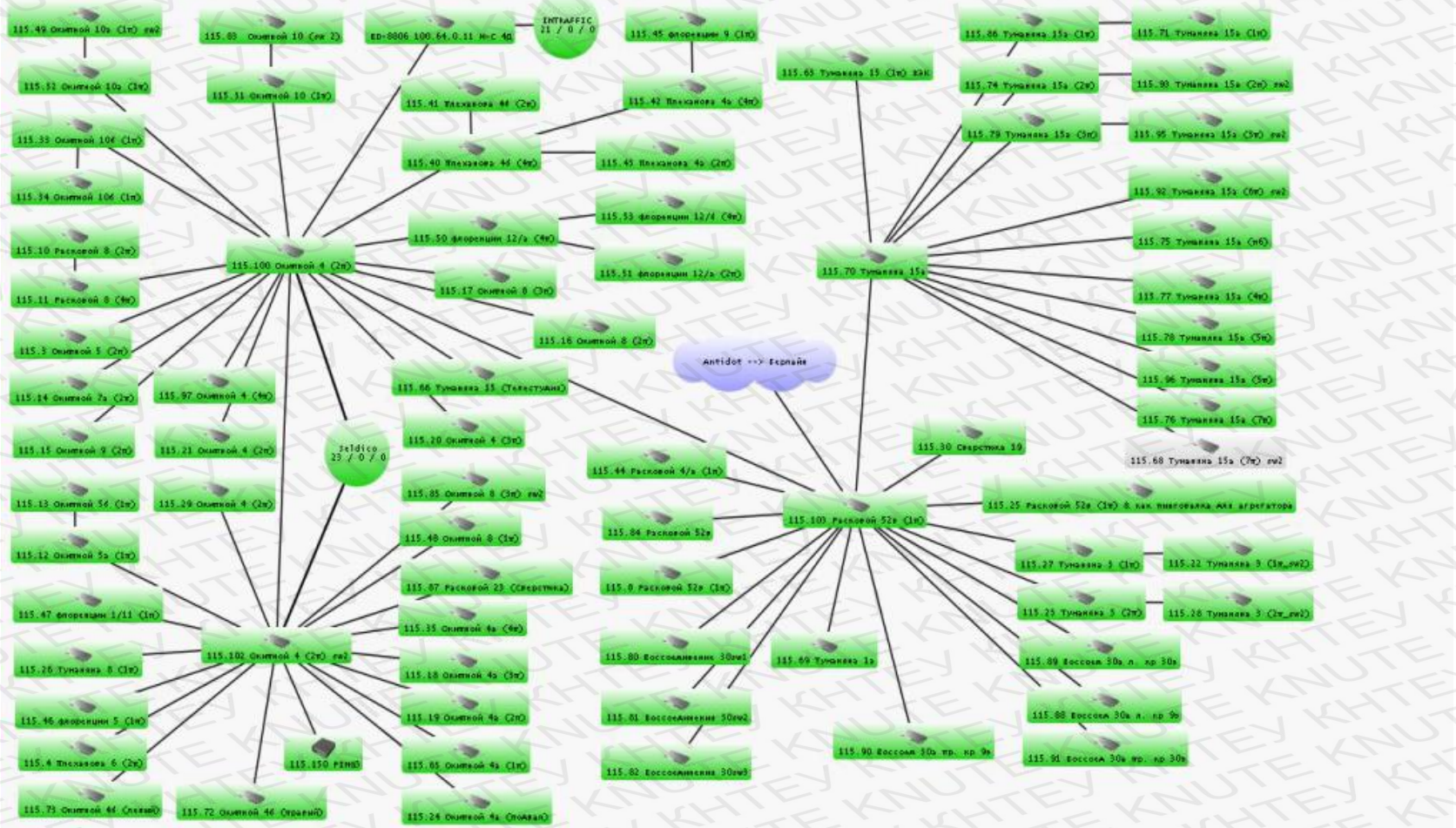
Графічна модель «Ядра м ережі» ТОВ «Intraffic»



Графічна модель ділянки мережі ТОВ «Intraffic» до стику з одним із партнерів



Графічна модель однієї з найобширніших ділянок мережі ТОВ «Intraffic», та L2-транспорт до одного з партнерів



Фрагмент конфігурації L3-комутатора Extream BD-8806

```
#
configure snmp sysName "100.64.0.11.intraffic"
configure snmp sysLocation "N-S-4D"
configure snmp sysContact "noc@intraffic.ua_(097)305-29-30"
configure timezone name Kiev 120 autodst name Kiev begins every last sunday march at 3 0 ends every
last sunday october at 4 0
configure slot 1 module 10G4Xc
configure sys-recovery-level slot 1 reset
configure slot 2 module 8900-10G24X-c
configure sys-recovery-level slot 2 reset
configure slot 6 module G48Xc
configure sys-recovery-level slot 6 reset
#
# Module vlan configuration.
#
configure vlan default delete ports all
configure vr VR-Default delete ports 1:1-4,2:1-24,6:1-48
configure vr VR-Default add ports 1:1-4,2:1-24,6:1-48
create vlan "subvlan_2009_34161"
configure vlan subvlan_2009_34161 tag 2009
create vlan "subvlan_2017_39300"
configure vlan subvlan_2017_39300 tag 2017
configure ports 1:3 display-string 100.64.0.16p.27_Down
configure ports 1:4 display-string 100.64.0.17_p.25_Dow
configure ports 1:4 description-string "100.64.0.17_p.25_DownLINK"
configure ports 2:1 display-string 111.102.intraffic
configure ports 2:1 auto off speed 10000 duplex full
configure ports 2:2 display-string 112.102.intraffic
configure ports 2:2 auto off speed 10000 duplex full
configure ports 2:3 display-string 113.102.intraffic
configure ports 2:3 auto off speed 10000 duplex full
configure ports 2:4 auto off speed 10000 duplex full
configure ports 2:5 auto off speed 10000 duplex full
configure ports 2:6 auto off speed 10000 duplex full
configure ports 2:7 auto off speed 10000 duplex full
configure ports 2:8 auto off speed 10000 duplex full
configure ports 2:24 display-string 100.64.0.14p.26_UPLI
configure ports 2:24 auto off speed 10000 duplex full
configure port 6:1 isolation on
configure ports 6:1 display-string abon-34161
configure port 6:1 rate-limit flood broadcast 5000
configure port 6:1 rate-limit flood multicast 5000
configure port 6:1 rate-limit flood unknown-destmac 5000
configure port 6:2 isolation on
configure ports 6:2 display-string 116.63.intraffic
configure port 6:3 isolation on
configure port 6:19 isolation on
configure ports 6:19 display-string 116.24.intraffic
configure port 6:20 isolation on
configure ports 6:20 display-string 116.23.intraffic
configure ports 6:21 display-string 116.25.intraffic
configure ports 6:22 display-string 116.17.intraffic
configure port 6:33 rate-limit flood unknown-destmac 5000
configure ports 6:34 display-string BGNet_Raskov_11
configure port 6:34 rate-limit flood broadcast 5000
configure ports 6:46 display-string 116.26.intraffic
configure ports 6:47 display-string 116.29.intraffic
```

```
configure ports 6:48 display-string School
configure vlan in-319-chereda-cli add ports 1:1-2,1:4,2:24 tagged
configure vlan subvlan_1495_38052 add ports 1:3,2:22 tagged
configure vlan subvlan_1503_36236 add ports 1:3,2:23 tagged
configure vlan subvlan_1510_39067 add ports 1:3,2:22 tagged
configure vlan subvlan_2002 add ports 1:3,2:21 tagged
configure vlan vlan-1119-pa-ukrbud add ports 2:24,6:29 tagged
configure vlan vlan-16-in ipaddress 100.76.0.1 255.255.252.0
enable ipforwarding vlan vlan-16-in
configure vlan vlan-16-in add secondary-ipaddress 91.218.72.1 255.255.255.0
configure vlan vlan-16-in add secondary-ipaddress 91.218.73.1 255.255.255.0
configure vlan vlan-16-in add secondary-ipaddress 91.218.74.1 255.255.255.0
configure vlan vlan-16-in add secondary-ipaddress 91.218.75.1 255.255.255.0
configure vlan vlan-116-in ipaddress 192.168.116.1 255.255.255.0
enable ipforwarding vlan vlan-116-in
configure vlan "vlan-1006-test-supervlan" add subvlan "vlan-2060-test-subvlan"
configure vlan "vlan-1007-test-supervlan" add subvlan "vlan-2061-test-subvlan"
#
configure radius mgmt-access primary server 94.232.215.29 1812 client-ip 100.64.0.11 vr VR-Default
configure radius mgmt-access primary shared-secret encrypted "3}hpP@S%"
configure radius mgmt-access secondary server 100.64.0.10 1812 client-ip 100.64.0.11 vr VR-Default
configure radius mgmt-access secondary shared-secret encrypted "3}hpP@S%"
enable radius mgmt-access
#
# Module elrp configuration.
#
#
# Module ems configuration.
#
configure syslog add 94.232.215.21:514 vr VR-Default local6
enable log target syslog 94.232.215.21:514 vr VR-Default local6
configure log target syslog 94.232.215.21:514 vr VR-Default local6 filter DefaultFilter severity Debug-
Data
configure log target syslog 94.232.215.21:514 vr VR-Default local6 match Any
configure log target syslog 94.232.215.21:514 vr VR-Default local6 format timestamp seconds date
Mmm-dd event-name none priority host-name tag-name

#
# Module netTools configuration.
#
configure dns-client add name-server 94.232.215.2 vr VR-Default
configure dns-client add name-server 100.64.0.250 vr VR-Default
configure dns-client add domain-suffix intraffic.ua
configure sntp-client primary 94.232.215.27 vr VR-Default
configure sntp-client secondary 94.232.215.28 vr VR-Default
configure sntp-client update-interval 3600
enable sntp-client
configure bootprelay dhcp-agent information option vr VR-Default
configure bootprelay dhcp-agent information policy keep vr VR-Default
enable bootprelay ipv4 vlan vlan-16-in
configure bootprelay vlan vlan-16-in add 100.64.0.20
configure bootprelay vlan vlan-16-in add 100.64.0.10
configure bootprelay vlan vlan-16-in dhcp-agent information option on

configure ospf routerid 100.64.0.11
disable ospf capability opaque-lsa
enable ospf
create ospf area 100.64.0.0
```

```
configure ospf add vlan vlan-1006-test-supervlan area 100.64.0.0 passive
configure ospf add vlan vlan-1007-test-supervlan area 100.64.0.0 passive
configure ospf add vlan vlan-116-in area 100.64.0.0 passive
configure ospf add vlan vlan-16-in area 100.64.0.0 passive
configure ospf add vlan vlan-207-ospf area 100.64.0.0
#
# Module ospfv3 configuration.
configure snmpv3 add group "v1v2cNotifyGroup" user "v1v2cNotifyUser1" sec-model snmpv2c
configure snmpv3 add community "v1v2cNotifyComm1" name "public" user "v1v2cNotifyUser1"
configure snmpv3 add target-addr "v1v2cNotifyTAddr1" param "v1v2cNotifyParam1" ipaddress
100.64.0.24 transport-port 162 tag-list "defaultNotify"
configure snmpv3 add target-params "v1v2cNotifyParam1" user "v1v2cNotifyUser1" mp-model snmpv2c
sec-model snmpv2c sec-level noauth
configure snmp access-profile "allow_subnet_mng" readwrite
#
configure ssl certificate hash-algorithm sha512

#
# Module twamp configuration.
#

#
# Module upm configuration.
#
create upm profile backup-config
# Work Around entry for loop protection
disable clip
#enable cli scripting
disable cli scripting output
#####
# Configurable Variables for use
#####
set var tftp 100.64.0.250
set var vrtr VR-Default
#####
# Start Functions
#####
set var cli.out 0
ls
set var lslist $tcl(split ${cli.out} "\n")
set var lslistlen $tcl(llength $lslist)
#debug
#show var lslist
#show var lslistlen
#####
# Getting your selected config for individual backup
#####
set var cli.out 0
show switch
set var slist $tcl(split ${cli.out} "\n")
set var slistsearch $tcl(lsearch -regexp $slist {Config Selected:})
set var slist $tcl(lindex $slist $slistsearch)
set var slist $tcl(split $slist " ")
set var slistsearch $tcl(lsearch -regexp $slist {.cfg})
set var slist $tcl(lindex $slist $slistsearch)
set var sysname $tcl(split ${cli.out} "\n")
set var sysname $tcl(lindex $sysname 1)
set var sysname $tcl(split $sysname " ")
```

```
set var sysname $tcl(lindex $sysname 10)
#####
# Getting System Time
#####
#_z_192.168.111.21_2019.01.30_014639.cfg
set var baseSystemTime $TCL(clock seconds)
set var systemTime $TCL(clock format $baseSystemTime -format {%Y.%m.%d_%H%M%S})
#debug
#show var systemTime
#show var sysname
#####
# Doing some string manipulation and formatting
#####
set var r_filename $(sysname)_$(systemTime)
#debug
#show var r_filename
upload configuration $tftp _config_$(r_filename).xsf vr $vrtr
if ($STATUS == 0) then
   create log entry "Backup configuration is OK"
else
   create log entry "Backup configuration is FAIL"
endif
tftp put $tftp vr $vrtr $slist _$(slist)_$(r_filename).cfg
if ($STATUS == 0) then
   create log entry "Backup Config[Selected] is OK"
else
   create log entry "Backup Config[Selected] is FAIL"
endif
set var count 0
while ($count < $lslistlen) do
set var curr $tcl(lindex $lslist $count)
set var curr $tcl(split $curr " ")
set var currlen $tcl(llength $curr)
set var currlen ($currlen - 1)
set var curr $tcl(lindex $curr $currlen)
####
# Getting all policies
####
set var tmpcfg $tcl(regexp -all {.pol} $curr)
if ($tmpcfg) then
        tftp put $tftp vr $vrtr $curr _$(curr)_$(r_filename).pol
        if ($STATUS == 0) then
           create log entry "Backup $(curr) is OK"
        else
           create log entry "Backup $(curr) is FAIL"
        endif
endif
####
# Getting all scripts
####
set var tmpcfg $tcl(regexp -all {.xsf} $curr)
if ($tmpcfg) then
        tftp put $tftp vr $vrtr $curr _$(curr)_$(r_filename).xsf
        if ($STATUS == 0) then
           create log entry "Backup $(curr) is OK"
        else
           create log entry "Backup $(curr) is FAIL"
        endif
```

```
endif
set var count ($count + 1)
endwhile
create log message "Files uploaded successfully to server $(tftp)"
del var cli.out
del var count
del var tmpcfg
del var curr
del var currlen
del var r_filename
del var systemTime
del var baseSystemTime
del var sysname
del var slist
del var slistsearch
del var lslistlen
del var lslist
del var tftp
del var vrtr
.
configure upm profile backup-config maximum execution-time 300
create upm timer backup-config-timer
configure upm timer backup-config-timer profile backup-config
configure upm timer backup-config-timer after 43200 every 86400
```

Фрагмент конфігурації L3-комутатора DGS-3620-28SC

```
#------------------------------------------------------------------------
#                DGS-3620-28SC Gigabit Ethernet Switch
#                        Configuration
#
#                     Firmware: Build 3.01.R003
#          Copyright(C) 2018 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------

# STACK

config stacking force_master_role state disable

# DEVICE

config temperature threshold high 79
config temperature threshold low 11
config temperature trap state enable
config temperature log state enable

# BASIC

# ACCOUNT LIST
create account admin bk
*@&FvwUDN7SJcmWic8f5x2zQWQWdFbXjDCL
*@&FvwUDN7SJcmWic8f5x2zQWQWdFbXjDCL

# ACCOUNT END
# PASSWORD ENCRYPTION
enable password encryption
config serial_port auto_logout 10_minutes
disable web
enable clipaging
config terminal width 80
enable command logging
enable password_recovery

# DEBUG

debug config state enable
debug config error_reboot enable

# STORM

config traffic control 1 broadcast disable multicast disable unicast disable action drop broadcast_threshold
131072 multicast_threshold 131072 unicast_threshold 131072 countdown 0 time_interval 5
config traffic control 2 broadcast disable multicast disable unicast disable action drop broadcast_threshold
131072 multicast_threshold 131072 unicast_threshold 131072 countdown 0 time_interval 5
config traffic control 3 broadcast disable multicast disable unicast disable action drop broadcast_threshold
131072 multicast_threshold 131072 unicast_threshold 131072 countdown 0 time_interval 5
config traffic control 4 broadcast disable multicast disable unicast disable action drop broadcast_threshold
131072 multicast_threshold 131072 unicast_threshold 131072 countdown 0 time_interval 5
config traffic control auto_recover_time 0
config traffic trap none
config traffic control log state enable
```

```
config sim candidate
config sim dp_interval 30
config sim hold_time 100

# GM_H

# MIRROR

create mirror group_id 1
config mirror group_id 1 target_port 26
config mirror group_id 1 state disable
disable mirror

# QOS

enable hol_prevention
config 802.1p default_priority 1-28 0
config bandwidth_control 1-28 rx_rate no_limit tx_rate no_limit
config per_queue bandwidth_control ports 1-28 0 min_rate  no_limit  max_rate no_limit
config per_queue bandwidth_control ports 1-28 1 min_rate  no_limit  max_rate no_limit
config per_queue bandwidth_control ports 1-28 6 min_rate  no_limit  max_rate no_limit
config per_queue bandwidth_control ports 1-28 7 min_rate  no_limit  max_rate no_limit
config scheduling_mechanism ports 1-28 strict
config scheduling ports 1-28 0  weight 1
config scheduling ports 1-28 1  weight 2
config scheduling ports 1-28 2  weight 3
config scheduling ports 1-28 3  weight 4
config scheduling ports 1-28 4  weight 5
config 802.1p user_priority ports 1-28 4  4
config 802.1p user_priority ports 1-28 5  5
config 802.1p user_priority ports 1-28 6  6
config 802.1p user_priority ports 1-28 7  7

# SYSLOG

config log_save_timing on_demand
enable syslog
config system_severity trap information
config system_severity log information
create syslog host 2 ipaddress 100.64.0.115 severity debug facility local6 udp_port 514 state enable
create syslog host 3 ipaddress 94.232.215.28 severity debug facility local6 udp_port 514 state enable
create syslog host 4 ipaddress 192.168.114.254 severity debug facility local6 udp_port 514 state enable
config syslog source_ipif System

# PFC

# TRAF-SEGMENTATION

config traffic_segmentation 1-4,7-8,10-16,18-21 forward_list 25-28
config traffic_segmentation 5,25-28 forward_list all
config traffic_segmentation 6 forward_list 17,25-28
config traffic_segmentation 9,22-24 forward_list 1-10,12-28
config traffic_segmentation 17 forward_list 6,25-28

# SSL

disable ssl
```

```
disable ssl version ssl3.0
enable ssl version tls1.0
enable ssl version tls1.1
enable ssl version tls1.2
disable ssl ciphersuite RSA_with_RC4_128_MD5
enable ssl ciphersuite RSA_with_3DES_EDE_CBC_SHA
enable ssl ciphersuite DHE_DSS_with_3DES_EDE_CBC_SHA
disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
enable ssl ciphersuite RSA_with_AES_128_CBC_SHA
enable ssl ciphersuite RSA_with_AES_256_CBC_SHA
enable ssl ciphersuite RSA_with_AES_128_CBC_SHA256
enable ssl ciphersuite RSA_with_AES_256_CBC_SHA256
enable ssl ciphersuite DHE_DSS_with_AES_256_CBC_SHA
enable ssl ciphersuite DHE_RSA_with_AES_256_CBC_SHA
config ssl cachetimeout 600

# PORT

enable jumbo_frame
config jumbo_frame ports 1-28 state enable
config ports 1-3,5-20 speed auto  capability_advertised  1000_full  auto_negotiation
remote_fault_advertised disable flow_control disable learning enable state enable
config ports 4 speed auto  capability_advertised  1000_full  auto_negotiation remote_fault_advertised
disable flow_control disable learning enable state enable description Dragomirova_2A_Pautina
config ports 21-24 medium_type copper speed auto  capability_advertised  10_half 10_full 100_half
100_full 1000_full flow_control disable learning enable state enable mdix auto
config ports 21-24 auto_speed_downgrade disable
config ports 21-24 medium_type fiber speed auto  capability_advertised  1000_full  auto_negotiation
remote_fault_advertised disable flow_control disable learning enable state enable
config ports 25-26 speed auto   flow_control disable learning enable state enable
config ports 27-28 speed auto   flow_control disable learning enable state enable description 27-
Patona;28-Metro

# SFLOW

enable sflow
create sflow analyzer_server 1 owner nfsen timeout infinite collectoraddress 100.64.0.117 collectorport
6314 maxdatagramsize 1400
create sflow flow_sampler ports 1-24 analyzer_server_id 1 rate 128 tx_rate 128 maxheadersize 128
create sflow counter_poller ports 1-24 analyzer_server_id 1 interval 20

# OAM

# DDM

config ddm trap enable
config ddm log enable
config ddm power_unit dbm
config ddm ports 1-28 state enable shutdown none

# MANAGEMENT

create trusted_host network 94.232.215.0/27 snmp ssh
create trusted_host network 10.10.10.0/24 snmp ssh
create trusted_host network 100.64.0.0/24 snmp ssh
enable snmp traps
enable snmp authenticate_traps
enable snmp linkchange_traps
```

```
enable snmp
config snmp system_name 100.64.0.14.intraffic
config snmp system_location Davidova, 2/7
config snmp system_contact (044)200-44-00,0-800-202-800
config snmp linkchange_traps ports 1-28 enable

# TRAP

config snmp coldstart_traps enable
config snmp warmstart_traps enable
config rmon trap rising_alarm enable
config rmon trap falling_alarm enable

# TR

# PortGroup

# IGMP_MULTICAST_VLAN

config igmp_snooping multicast_vlan forward_unmatched disable
config igmp_snooping multicast_vlan auto_assign_vlan disable

# MLD_MULTICAST_VLAN

config mld_snooping multicast_vlan forward_unmatched disable
config mld_snooping multicast_vlan auto_assign_vlan disable

# VLAN

enable pvid auto_assign
config vlan default delete 1-28
config vlan default advertisement enable
create vlan 11 tag 11
config vlan 11 add tagged 1-2,25-28 advertisement disable
create vlan 12 tag 12
create vlan 17 tag 17
config vlan 17 add tagged 1-2,25-28 advertisement disable
create vlan 18 tag 18
config vlan 18 add tagged 1-2,25-28 advertisement disable

create vlan vlan-3896-in-39981 tag 3896
config vlan vlan-3896-in-39981 add tagged 26 advertisement disable
create vlan vlan-3897-in-38619 tag 3897
config vlan vlan-3897-in-38619 add tagged 26 advertisement disable
disable gvrp
disable asymmetric_vlan
disable vlan_trunk
config port_vlan 1-5,7-23,25-28 gvrp_state disable ingress_checking enable acceptable_frame admit_all
pvid 1
config port_vlan 6 gvrp_state disable ingress_checking enable acceptable_frame admit_all pvid 14
config port_vlan 24 gvrp_state disable ingress_checking enable acceptable_frame admit_all pvid 114

# URPF

# PORT_SECURITY

config port_security system max_learning_addr no_limit
config port_security trap state disable
```

```
config port_security log state disable
config port_security ports 1-28 admin_state disable max_learning_addr 32 action drop
lock_address_mode deleteonreset

# ACL

create access_profile profile_id 1 profile_name deny ethernet source_mac FF-FF-FF-FF-FF-FF
ethernet_type
config access_profile profile_id 1 add access_id 1 ethernet source_mac 00-00-00-00-00-00 mask FF-FF-
FF-FF-FF-FF port 1-24 deny
config access_profile profile_id 1 add access_id 2 ethernet ethernet_type 0x86DD port 1-24,26-28 deny
create access_profile profile_id 2 profile_name pve ip source_ip_mask 255.255.255.255
config access_profile profile_id 2 add access_id auto_assign ip source_ip 10.10.10.92 port 27-28 permit
priority 7 replace_priority urpf_state_check enable
config access_profile profile_id 4 add access_id auto_assign ip vlan_id 1000 destination_ip 192.168.0.0
mask 255.255.0.0 port 1-28 deny
config access_profile profile_id 4 add access_id auto_assign ip vlan_id 1001 destination_ip 192.168.0.0
mask 255.255.0.0 port 1-28 deny

#CPU Interface Filter

disable cpu_interface_filtering

# SUBNETVLAN

config vlan_precedence port 1-28 mac_based_vlan

# PROTOCOL_VLAN

# PowerSaving

config power_saving mode link_detection enable
config power_saving mode length_detection disable
config power_saving mode hibernation disable
config power_saving mode led disable
config power_saving mode port disable

# LED-CTRL

config led state enable

# QINQ

# manaport

config out_band_ipif  ipaddress 192.168.0.1/24
config out_band_ipif  state enable
config out_band_ipif  gateway 0.0.0.0

# ExternalAlarm

config external_alarm unit 1 channel 1 message External Alarm 1
config external_alarm unit 1 channel 2 message External Alarm 2
config external_alarm unit 2 channel 1 message External Alarm 3
config external_alarm unit 2 channel 2 message External Alarm 4
config external_alarm unit 11 channel 2 message External Alarm 22
config external_alarm unit 12 channel 1 message External Alarm 23
config external_alarm unit 12 channel 2 message External Alarm 24
```

SUPERVLAN

create super_vlan vlanid 1000
create super_vlan vlanid 1001
config super_vlan vlanid 1001 add sub_vlan 319
config super_vlan vlanid 1001 add sub_vlan 933
config super_vlan vlanid 1001 add sub_vlan 935-936
config super_vlan vlanid 1001 add sub_vlan 948-951
config super_vlan vlanid 1001 add sub_vlan 961
config super_vlan vlanid 1001 add sub_vlan 2101
config super_vlan vlanid 1001 add sub_vlan 2119
config super_vlan vlanid 1001 add sub_vlan 2248

RSPAN

disable rspan

8021X

disable 802.1x
config 802.1x trap state disable
config 802.1x auth_protocol radius_eap
config 802.1x fwd_pdu system disable
config 802.1x max_users 448
config 802.1x authorization attributes radius enable
config 802.1x capability ports 1-28 none
config 802.1x auth_parameter ports 1-28 direction both port_control auto quiet_period 60 tx_period 30 supp_timeout 30 server_timeout 30 max_req 2 reauth_period 3600 enable_reauth disable
config 802.1x auth_parameter ports 1-28 max_users 16

guestvlan

NLB

MCFDB

FDB

config fdb aging_time 300
config fdb vlan_learning vlanid 1,11-14,16-19,33-34,100-101,111-119,122,206-208,318-322,333,371,430-433,501,504,712,731,807-808,839-844,851-853,860,865,870,875-876,880-883,885,932-937,948-951,961,964-969,971-984,986-990,992,998,1000-1001,1004,1049,1079-1082,1088-1094,1097-1098,1119,1134,1150,1152-1153,1216,1276,1281,1302,1335,1341-1342,1350,1360,1505,1509,1599-1600,1617,1777,1881-1882,1998,2005,2019,2021-2024,2026-2030,2035-2036,2040-2043,2045-2046,2049-2051,2061-2063,2075,2080,2082-2088,2090-2102,2110-2119,2159,2248,2705-2706,3344,3610-3621,3628-3630,3700,3896-3897 state enable
debug fdb config algorithm dual
debug fdb config hash_table l2_hash algorithm crc32_lower
debug fdb config hash_table dual_hash algorithm crc32_upper

VLANCounter

ADDRBIND

config address_binding dhcp_snoop max_entry ports 1 limit no_limit
config address_binding dhcp_snoop max_entry ports 2 limit no_limit
config address_binding dhcp_snoop max_entry ports 3 limit no_limit

```
config address_binding dhcp_snoop max_entry ports 4 limit no_limit
config address_binding dhcp_snoop max_entry ports 5 limit no_limit
config address_binding dhcp_snoop max_entry ports 6 limit no_limit
config address_binding dhcp_snoop max_entry ports 7 limit no_limit
config address_binding dhcp_snoop max_entry ports 27 limit no_limit
config address_binding dhcp_snoop max_entry ports 28 limit no_limit
disable address_binding dhcp_snoop
disable address_binding trap_log
enable address_binding roaming
config address_binding dhcp_snoop_entry filename /d:/dhcpsnp.cfg autosave enable
config address_binding dhcp snooping recovery_timer 300
disable address_binding dhcp_snoop ipv6
disable address_binding nd_snoop
config address_binding dhcp_snoop max_entry ports 1-28 limit no_limit ipv6
config address_binding nd_snoop ports 1-28 max_entry no_limit

# NetBiosFilter

config filter netbios all state disable
config filter netbios 1-4,6-28 state enable
config filter extensive_netbios all state disable
config filter extensive_netbios 1-4,6-28 state enable

# RADIUS

# DoS

config dos_prevention dos_type land_attack action drop state enable
config dos_prevention dos_type blat_attack action drop state enable
config dos_prevention trap enable
config dos_prevention log disable

# DhcpServerScreening

config filter dhcp_server ports all state disable
config filter dhcp_server ports 5,7-8,10-24 state enable
config filter dhcp_server illegal_server_log_suppress_duration 5min
config filter dhcp_server trap enable
config filter dhcp_server log enable

# sRED

config dscp trust all state disable
config dscp map all dscp_dscp 0 to 0
config dscp map all dscp_dscp 1 to 1
config dscp map all dscp_dscp 2 to 2
config dscp map all dscp_dscp 3 to 3
config dscp map all dscp_dscp 39 to 39
config dscp map all dscp_dscp 40 to 40
config dscp map all dscp_dscp 62 to 62
config dscp map all dscp_dscp 63 to 63
config dscp map all dscp_priority 0-7 to 0
config dscp map all dscp_priority 8-15 to 1
config dscp map all dscp_priority 16-23 to 2
config dscp map all dscp_priority 24-31 to 3
config dscp map all dscp_priority 32-39 to 4
config dscp map all dscp_priority 40-47 to 5
config dscp map all dscp_priority 48-55 to 6
```

```
config dscp map all dscp_priority 56-63 to 7

# FilterIPv6

config filter dhcpv6_server trap disable
config filter dhcpv6_server log enable
config filter icmpv6_ra_all_node trap disable
config filter icmpv6_ra_all_node log enable

# ARPSpoofingPrevention

# WRED

config wred profile default tcp green min_threshold 50 max_threshold 100 max_drop_rate 50
config wred profile default tcp yellow min_threshold 50 max_threshold 100 max_drop_rate 50
config wred profile default tcp red min_threshold 50 max_threshold 100 max_drop_rate 50
config wred profile default non_tcp green min_threshold 50 max_threshold 100 max_drop_rate 50
config wred profile default non_tcp yellow min_threshold 50 max_threshold 100 max_drop_rate 50
config wred profile default non_tcp red min_threshold 50 max_threshold 100 max_drop_rate 50
disable wred
config wred ports 1-28 cos 0 profile default
config wred ports 1-28 cos 0 weight 9
config wred ports 1-28 cos 1 profile default
config wred ports 1-28 cos 1 weight 9
config wred ports 1-28 cos 2 profile default
config wred ports 1-28 cos 2 weight 9
config wred ports 1-28 cos 3 profile default
config wred ports 1-28 cos 3 weight 9
config wred ports 1-28 cos 4 profile default
config wred ports 1-28 cos 4 weight 9
config wred ports 1-28 cos 5 profile default
config wred ports 1-28 cos 5 weight 9
config wred ports 1-28 cos 6 profile default
config wred ports 1-28 cos 6 weight 9
config wred ports 1-28 cos 7 profile default
config wred ports 1-28 cos 7 weight 9

# MAC_ADDRESS_TABLE_NOTIFICATION

disable mac_notification
config mac_notification interval 1 historysize 50
config mac_notification ports 1-28 disable

# STP

 config stp version rstp
 config stp maxage 20 maxhops 20 forwarddelay 15 txholdcount 6 fbpdu disable hellotime 2
nni_bpdu_addr dot1d
 config stp priority 32768 instance_id 0
 config stp ports 1-28 externalCost auto  edge false p2p auto state enable restricted_role false
restricted_tcn false
 config stp mst_ports 1-28 instance_id 0 internalCost auto priority 128
config stp ports 1-28 fbpdu disable
 config stp mst_config_id name FC:75:16:37:DE:00 revision_level 0
 config stp trap new_root enable
 config stp trap topo_change  enable
 disable stp
```

```
# L2PT

disable l2protocol_tunnel
config l2protocol_tunnel ports all type none

# BPDU_PROTECTION

config bpdu_protection ports 1-28 mode shutdown

# SAFEGUARD_ENGINE

config safeguard_engine state enable utilization rising 95 falling 80 trap_log disable mode fuzzy

# BANNER_PROMP

config command_prompt DGS-3620-28_2/7
config greeting_message default

# SSH

 config ssh algorithm 3DES enable
 config ssh algorithm AES128 enable
 config ssh algorithm AES192 enable
 config ssh algorithm AES256 enable
 config ssh algorithm arcfour enable
 config ssh algorithm blowfish enable
 config ssh algorithm cast128 enable
 config ssh algorithm twofish128 enable
 config ssh algorithm twofish192 enable
 config ssh algorithm twofish256 enable
 config ssh algorithm MD5 enable
 config ssh algorithm SHA1 enable
 config ssh algorithm RSA enable
 config ssh algorithm DSA enable
 config ssh authmode password enable
 config ssh authmode publickey enable
 config ssh authmode hostbased enable
 config ssh server maxsession 8
 config ssh server contimeout 600
 config ssh server authfail 2
 config ssh server rekey never
 config ssh server port 22
 config ssh user bk authmode password
 config ssh publickey bypass_login_screen state disable
 enable ssh

# SFTPS

 config sftp server timeout 120
 disable sftp server

# SERVER_PROFILE

# TELNETS

disable telnet

# DNSRESOLVER
```

```
disable dns_resolver
config name_server timeout 3

# BCPING

enable broadcast_ping_reply

# NTP

disable ntp
config ntp authentication state enable
config ntp update-calendar state disable
config ntp access_group add default nomodify noquery
config ntp max_associations 32

# SNTP

enable sntp
config time_zone operator + hour 2 min 0
config sntp primary 94.232.215.27 secondary 94.232.215.28 poll-interval 3600
config dst annual s_date 29 s_mth 4 s_time 0:0 e_date 12 e_mth 10 e_time 0:0 offset 60
config dst repeating s_week last s_day sun s_mth 3 s_time 3:0 e_week last e_day sun e_mth 10 e_time
4:0 offset 60

# MULTICAST_FILTER

# LACP

config link_aggregation algorithm ip_source_dest
create link_aggregation group_id 1 type lacp
config link_aggregation group_id 1 master_port 1 ports 1-2 state enable
config link_aggregation group_id 1 trap enable
create link_aggregation group_id 2 type lacp
config link_aggregation group_id 2 master_port 27 ports 27-28 state enable
config link_aggregation group_id 2 trap enable
config lacp_port 1-4,27-28 mode active lacp_timeout short
config lacp_port 5-26 mode passive lacp_timeout short

# IP

config ipif System ipaddress 100.64.0.14/24 vlan 207
config ipif System ipv6 state disable
config ipif System dhcpv6_client disable
config ipif System dhcpv6_client_pd disable
config ipif System proxy_arp disable local disable
config ipif 13 dhcpv6_client_pd disable
config ipif_mac_mapping ipif 111 mac_offset 8
create ipif 111 192.168.111.1/24 111 state enable
pping ipif svi-1000 mac_offset 0
create ipif svi-1000 94.232.214.1/25 svi-1000 state enable
config ipif svi-1000 proxy_arp disable local disable
config ipif svi-1000 ipv6 state disable
config ipif svi-1000 dhcpv6_client disable
config ipif svi-1000 dhcpv6_client_pd disable
config ipif_mac_mapping ipif svi-1001 mac_offset 2
create ipif svi-1001 94.232.214.129/25 svi-1001 state enable
config ipif svi-1001 proxy_arp disable local disable
```

```
config ipif svi-1001 ipv6 state disable
config ipif svi-1001 dhcpv6_client disable
config ipif svi-1001 dhcpv6_client_pd disable
create ipif 14 100.74.0.1/22 14 state enable secondary
config ipif 14 proxy_arp disable local disable
create ipif 11_r1 94.232.211.1/24 11 state enable secondary
config ipif 13_r2 proxy_arp disable local disable
create ipif 14_r2 91.197.171.129/25 14 state enable secondary
config ipif 14_r2 proxy_arp disable local disable
create ipif svi-1000-nat 100.70.0.1/22 svi-1000 state enable secondary
config ipif svi-1000-nat proxy_arp disable local disable
create ipif svi-1001-nat 100.70.4.1/22 svi-1001 state enable secondary
config ipif svi-1001-nat proxy_arp disable local disable
config ipif 11 ip_mtu 1500
config ipif 12 ip_mtu 1500
config ipif 13 ip_mtu 1500
config ipif 111 ip_mtu 1500
config ipif 112 ip_mtu 1500
config ipif 113 ip_mtu 1500
config ipif 114 ip_mtu 1500
config ipif 122 ip_mtu 1500
config ipif 14_r1 ip_mtu 1500
config ipif System ip_mtu 1500
config ipif svi-1000 ip_mtu 1500
config ipif svi-1001 ip_mtu 1500
config ipif 11  ip_directed_broadcast  disable
config ipif 12  ip_directed_broadcast  disable
config ipif svi-1001-nat  ip_directed_broadcast  disable
config ipif System dhcp_option12 state disable
disable autoconfig

# SNMPv3

delete snmp community public
delete snmp community private
delete snmp user initial
delete snmp group initial
delete snmp view restricted all
delete snmp view CommunityView all
config snmp engineID 800000ab03fc751637de00
create snmp view restricted 1.3.6.1.2.1.1 view_type included
create snmp view restricted 1.3.6.1.2.1.11 view_type included
create snmp view restricted 1.3.6.1.6.3.10.2.1 view_type included
create snmp view restricted 1.3.6.1.6.3.11.2.1 view_type included
create snmp view restricted 1.3.6.1.6.3.15.1.1 view_type included
create snmp view CommunityView 1 view_type included
create snmp view CommunityView 1.3.6.1.6.3 view_type excluded
create snmp view CommunityView 1.3.6.1.6.3.1 view_type included
create snmp group public v1 read_view CommunityView notify_view CommunityView
create snmp group public v2c read_view CommunityView notify_view CommunityView
create snmp group initial v3  noauth_nopriv read_view restricted notify_view restricted
create snmp group private v1 read_view CommunityView write_view CommunityView notify_view
CommunityView
create snmp group private v2c read_view CommunityView write_view CommunityView notify_view
CommunityView
create snmp community private view CommunityView read_write
create snmp community public view CommunityView read_only
create snmp user initial initial
```

```
create snmp host 100.64.0.24 v2c  public  udp_port 162
disable community_encryption
config snmp udp_port 161
config snmp trap_port ports 1-28 state enable

# VOICEVLAN

# SURVEILLANCEVLAN

# SD_Card_Management

# ERPS

 create erps raps_vlan 100
 config erps raps_vlan 100 timer holdoff_time 0 guard_time 500 wtr_time 5
 config erps raps_vlan 100 rpl_port none
 config erps raps_vlan 100 rpl_owner disable
 config erps raps_vlan 100 ring_mel 1
config erps raps_vlan 100 revertive  enable
 config erps raps_vlan 100 ring_port west 25
 config erps raps_vlan 100 ring_port east 27
 create erps raps_vlan 101
 config erps raps_vlan 101 timer holdoff_time 0 guard_time 500 wtr_time 5
config erps raps_vlan 101 ring_port west virtual_channel
 config erps raps_vlan 101 ring_port east 26
 config erps raps_vlan 101 protected_vlan add vlanid 2001
 config erps raps_vlan 100 add sub_ring raps_vlan 101
 config erps raps_vlan 100 sub_ring raps_vlan 101 tc_propagation state enable
 config erps raps_vlan 100 state enable
 config erps raps_vlan 101 state enable
 enable erps
 config erps log enable
 config erps trap enable

# BFD

# IGMP_PROXY

config igmp_proxy upstream_if vlan vlanid 1
config igmp_proxy upstream_if source_ip 0.0.0.0

# MLD_PROXY

config mld_proxy upstream_if vlan vlanid 1
config mld_proxy upstream_if source_ip ::

# UDP_HELPER

disable udp_helper

# JWAC

config jwac switch_http_port 80
config jwac clear_quarantine_server_url
config jwac radius_protocol pap
disable jwac quarantine_server_monitor
config jwac quarantine_server_error_timeout 30
enable jwac forcible_logout
```

```
enable jwac udp_filtering
enable jwac redirect
config jwac redirect destination quarantine_server delay_time 1
disable jwac
config jwac authenticate_page english
config jwac authorization attributes radius enable
config jwac authorization attributes local enable
config jwac ports 1-28 max_authenticating_host 100 aging_time 1440 idle_time infinite block_time 60

# WAC

 config wac switch_http_port 80
 config wac method local
 config wac authorization attributes local enable
 config wac authorization attributes radius enable
 config wac trap state disable
 disable wac
 config wac authentication_page element login_window_title Authentication Login
 config wac authentication_page element user_name_title User Name
 config wac authentication_page element password_title Password
 config wac authentication_page element logout_window_title Logout From The Network
 config wac ports 1-28 aging_time 1440 idle_time infinite block_time 60

# LLDP

enable lldp
config lldp message_tx_interval 30
config lldp tx_delay 2
config lldp message_tx_hold_multiplier 4
config lldp reinit_delay 2
config lldp notification_interval 5
config lldp ports 25-28 dot1_tlv_protocol_identity eapol enable
config lldp ports 25-28 dot1_tlv_protocol_identity lacp enable
config lldp ports 25-28 dot1_tlv_protocol_identity gvrp enable
config lldp ports 25-28 dot1_tlv_protocol_identity stp enable
config lldp ports 25-28 dot3_tlvs mac_phy_configuration_status link_aggregation  maximum_frame_size
enable

# TELNETC

# LOOP_DETECT

enable loopdetect
config loopdetect recover_timer 60 interval 10 mode vlan-based
config loopdetect log state enable
config loopdetect ports 1 state enable
config loopdetect ports 2 state enable
config loopdetect ports 3 state enable
config loopdetect ports 4 state enable
config loopdetect ports 10 state enable
config loopdetect ports 11 state enable
config loopdetect ports 12 state enable
config loopdetect ports 27 state disable
config loopdetect ports 28 state disable
config loopdetect trap both

# TFTPC
```

MAC-based_Access_Control

disable mac_based_access_control
config mac_based_access_control authorization attributes radius enable local enable
config mac_based_access_control ports 1-28 state disable
config mac_based_access_control ports 3 max_users 1024
config mac_based_access_control ports 3 aging_time 1440
config mac_based_access_control ports 3 block_time 300
config mac_based_access_control ports 4 max_users 1024
config mac_based_access_control ports 4 aging_time 1440
config mac_based_access_control ports 15 block_time 300
config mac_based_access_control ports 16 max_users 1024
config mac_based_access_control ports 16 aging_time 1440
config mac_based_access_control ports 16 block_time 300
config mac_based_access_control ports 17 max_users 1024
config mac_based_access_control password_type manual_string
config mac_based_access_control max_users no_limit
config mac_based_access_control trap state enable
config mac_based_access_control log state enable

MCFILTER

config multicast vlan_filtering_mode vlanid 34 forward_all_groups
config multicast vlan_filtering_mode vlanid 1 filter_unregistered_groups
config multicast vlan_filtering_mode vlanid 11-14 filter_unregistered_groups
config multicast vlan_filtering_mode vlanid 1509 filter_unregistered_groups
config multicast vlan_filtering_mode vlanid 2023 filter_unregistered_groups
config multicast vlan_filtering_mode vlanid 2102 filter_unregistered_groups
config multicast vlan_filtering_mode vlanid 2705-2706 filter_unregistered_groups
config multicast vlan_filtering_mode vlanid 3344 filter_unregistered_groups
config multicast vlan_filtering_mode vlanid 3630 filter_unregistered_groups

COMPOUND_AUTHENTICATION

config authentication ports 1-28 auth_mode host_based
config authentication ports 1-28 multi_authen_methods none
enable authorization attributes
config authentication server failover block
config authentication mac_format case uppercase
config authentication mac_format delimiter none
config authentication mac_format delimiter number 5

LLDP-MED

config lldp_med fast_start repeat_count 4
config lldp_med log state disable
config lldp_med notification topo_change ports 1 state disable
config lldp_med notification topo_change ports 2 state disable
config lldp_med notification topo_change ports 16 state disable
config lldp_med notification topo_change ports 17 state disable
config lldp_med notification topo_change ports 18 state disable
config lldp_med notification topo_change ports 25 state disable
config lldp_med notification topo_change ports 26 state disable
config lldp_med notification topo_change ports 27 state disable
config lldp_med notification topo_change ports 28 state disable

IGMP_SNOOPING

enable igmp_snooping
config igmp_snooping vlan_name default topology_changes_notification process fast_leave disable proxy_reporting state disable source_ip 0.0.0.0 state enable
config igmp_snooping querier vlan_name default query_interval 125 max_response_time 10 robustness_variable 2 last_member_query_interval 1 state disable version 3
config igmp_snooping vlan_name 11 topology_changes_notification process fast_leave disable robustness_variable 2 last_member_query_interval 1 state disable version 3
config igmp_snooping vlan_name 16 topology_changes_notification process fast_leave disable proxy_reporting state disable source_ip 0.0.0.0 state enable
config igmp_snooping querier vlan_name 16 query_interval 125 max_response_time 10 robustness_variable 2 last_member_query_interval 1 state disable version 3
config igmp_snooping vlan_name 17 topology_changes_notification process fast_leave disable proxy_reporting state disable source_ip 0.0.0.0 state enable
LLDP-DCBX

MLDSNP

config mld_snooping vlan_name default topology_changes_notification process fast_done disable proxy_reporting state disable source_ip :: state disable
config mld_snooping querier vlan_name default query_interval 125 max_response_time 10 robustness_variable 2 last_listener_query_interval 1 state disable version 2
config mld_snooping vlan_name 11 topology_changes_notification process fast_done disable robustness_variable 2 last_listener_query_interval 1 state disable version 2
config mld_snooping vlan_name 16 topology_changes_notification process fast_done disable proxy_reporting state disable source_ip :: state disable
config mld_snooping querier vlan_name 16 query_interval 125 max_response_time 10 robustness_variable 2 last_listener_query_interval 1 state disable version 2

ACCESS_AUTHENTICATION_CONTROL

create radius server_host 94.232.215.29 auth_port 1812 acct_port 1813 encryption_key
create authen_login method_list_name rad_ext
config authen_login method_list_name rad_ext method radius local
config authen_enable default method local_enable
create authen_enable method_list_name rad_ext_ena
config authen_enable method_list_name rad_ext_ena method radius local_enable
config accounting default method none
config authen application console login method_list_name rad_ext
config authen application console enable method_list_name rad_ext_ena
config authen application http enable method_list_name rad_ext_ena
disable aaa_server_password_encryption
enable authen_policy
config authen parameter response_timeout 0
config authen parameter attempt 3
config admin local_enable encrypt sha_1 *@&2jmj7l5rSw0yVb/vlWAYkK/YBwmwMs6D
config accounting service network state disable
config accounting service shell state disable
config accounting service command power_user none
config accounting service command user none

DHCP_LOCAL_RELAY

disable dhcp_local_relay

PTP

disable ptp

```
config ptp mode e2e_transparent
config ptp transport protocol udp
config ptp boundary priority1 128 priority2 128
config ptp clock domain_number 0 unit 1
config ptp ports 1-28 state disable
config ptp boundary ports 1-28 sync_interval 1
config ptp boundary ports 1-28 delay_mechanism e2e
config ptp boundary ports 1-28 announce  interval 2 delay_req_interval 0 pdelay_req_interval 1
config ptp boundary ports 1-28 announce timeout 3
config ptp p2p_transparent ports 1-28 pdelay_req_interval 1

# AAA_LOCAL_ENABLE_PASSWORD

# AAA ADMIN PWD LIST
config admin local_enable encrypt sha_1 *@&2jmj7l5rSw0yVb/vlWAYkK/YBwmwMs6D
# AAA ADMIN PWD END

# NDP

config ipv6 nd ns ipif System retrans_time 0
config ipv6 nd ra ipif System state disable life_time 1800 reachable_time 1200000 retrans_time 0
hop_limit 64 managed_flag disable other_config_flag disable min_rtr_adv_interval 198
max_rtr_adv_interval 600
config ipv6 nd ns ipif 114 retrans_time 0
config ipv6 nd ra ipif 114 state disable life_time 1800 reachable_time 1200000 retrans_time 0 hop_limit
64 managed_flag disable other_config_flag disable min_rtr_adv_interval 198 max_rtr_adv_interval 600
config ipv6 nd ns ipif svi-1001 retrans_time 0
config ipv6 nd ra ipif svi-1001 state disable life_time 1800 reachable_time 1200000 retrans_time 0
hop_limit 64 managed_flag disable other_config_flag disable min_rtr_adv_interval 198
max_rtr_adv_interval 600

# ARP

debug arp config lpm table_size 0
debug arp config lpm state disable
debug arp config arp_collision_log state disable
debug config queueing_unknown_pkt state disable
config arp_aging time 20
config arp_retry times 4
config gratuitous_arp send ipif_status_up disable
config gratuitous_arp send dup_ip_detected disable
config gratuitous_arp learning enable

# ROUTEFILTER

# SNP_AUTH

# PROUTE

# ROUTE

config route preference static 60
config route preference rip 100
config route preference default 1
config route preference ospfIntra 80
config route preference ospfInter 90
config route preference ospfExt1 110
config route preference ospfExt2 115
```

```
create iproute default 100.64.0.200 1 primary
config ecmp algorithm ip_destination   crc_low
enable ecmp ospf

# RELAY6

config dhcpv6_relay hop_count  4
disable dhcpv6_relay
config dhcpv6_relay option_37 state disable check disable
config dhcpv6_relay option_37 remote_id default

# DHCPv6_SERVER

disable dhcpv6_server
config dhcpv6_server ipif 14_r1 state enable
config dhcpv6_server ipif svi-1000 state enable
config dhcpv6_server ipif 113 state enable
config dhcpv6_server ipif 114 state enable
config dhcpv6_server ipif 122 state enable

# FLEX_LINK

# IGMP

config igmp ipif System version 3 query_interval 125 max_response_time 10 robustness_variable 2 state
disable
config igmp ipif System last_member_query_interval 1
config igmp check_subscriber_source_network ipif System enable
config igmp ipif 111 last_member_query_interval 1
config igmp ipif 114 version 3 query_interval 125 max_response_time 10 robustness_variable 2 state
disable
config igmp ipif 114 last_member_query_interval 1
config igmp check_subscriber_source_network ipif 114 enable
config igmp ipif 122 version 3 query_interval 125 max_response_time 10 robustness_variable 2 state
disable
config igmp ipif 122 last_member_query_interval 1
config igmp check_subscriber_source_network ipif 122 enable
config igmp check_subscriber_source_network ipif svi-1000 enable
config igmp ipif svi-1001 version 3 query_interval 125 max_response_time 10 robustness_variable 2
state disable
config igmp ipif svi-1001 last_member_query_interval 1
config igmp check_subscriber_source_network ipif svi-1001 enable

# PIMSM

disable pim
config pim cbsr hash_masklen 30
config pim cbsr bootstrap_period 60
config pim register_suppression_time 60
config pim register_probe_time 5
config pim last_hop_spt_switchover never
config pim crp holdtime 150 priority 192
config pim crp wildcard_prefix_cnt 0
config pim-ssm state disable group_range 232.0.0.0/8

# IPMROUTE

# RIP
```

```
disable rip
config rip timers update 30 timeout 180 garbage_collection 120
config rip ipif System tx_mode disable state disable
config rip ipif System rx_mode disable state disable
config rip ipif System distribute_list_in none
config rip ipif l1 tx_mode disable state disable
config rip ipif l1 rx_mode disable state disable
config rip ipif l1 distribute_list_in none
config rip ipif l2 tx_mode disable state disable
config rip ipif l12 rx_mode disable state disable
config rip ipif l12 distribute_list_in none
config rip ipif l13 tx_mode disable state disable
config rip ipif l13 rx_mode disable state disable
config rip ipif l13 distribute_list_in none
config rip ipif l14 tx_mode disable state disable
config rip ipif l14 rx_mode disable state disable
config rip ipif l14 distribute_list_in none
config rip ipif svi-1000 distribute_list_in none
config rip ipif svi-1001 tx_mode disable state disable
config rip ipif svi-1001 rx_mode disable state disable
config rip ipif svi-1001 distribute_list_in none
config rip ipif l4 tx_mode disable state disable
config rip ipif l4 rx_mode disable state disable
config rip ipif l4 distribute_list_in none
config rip ipif l1_r1 tx_mode disable state disable
config rip ipif l1_r1 rx_mode disable state disable
config rip ipif l1_r1 distribute_list_in none
config rip ipif l2_r1 tx_mode disable state disable
config rip ipif l2_r1 rx_mode disable state disable
config rip ipif l2_r1 distribute_list_in none
config rip ipif l2_r2 tx_mode disable state disable
config rip ipif l2_r2 rx_mode disable state disable
config rip ipif svi-1000-nat rx_mode disable state disable
config rip ipif svi-1000-nat distribute_list_in none
config rip ipif svi-1001-nat tx_mode disable state disable
config rip ipif svi-1001-nat rx_mode disable state disable
config rip ipif svi-1001-nat distribute_list_in none

# MD5

# OSPF

create ospf area 100.64.0.0 type normal
config ospf ipif l3_r2 bfd disable
config ospf ipif l3_r2 area 100.64.0.0 priority 1 hello_interval 10 dead_interval 40
config ospf ipif l3_r2 authentication none metric 1 state enable passive disable
config ospf ipif l3_r2 distribute_list_in none
config ospf ipif l4_r2 bfd disable
config ospf ipif l4_r2 area 100.64.0.0 priority 1 hello_interval 10 dead_interval 40
config ospf ipif l4_r2 authentication none metric 1 state enable passive disable
config ospf ipif l4_r2 distribute_list_in none
config ospf ipif l4_r1 bfd disable
config ospf ipif l4_r1 area 100.64.0.0 priority 1 hello_interval 10 dead_interval 40
config ospf ipif l2_r1 distribute_list_in none
config ospf ipif svi-1000 bfd disable
passive disable
config ospf ipif l1 distribute_list_in none
```

```
config ospf ipif 111 authentication none metric 1 state enable passive disable
config ospf ipif 122 area 100.64.0.0 priority 1 hello_interval 10 dead_interval 40
config ospf ipif 122 authentication none metric 1 state enable passive disable
config ospf ipif 122 distribute_list_in none
config ospf default-information originate none mettype 2  metric 10
config ospf router_id 100.64.0.14
enable ospf

# DNSR

disable dnsr
config dnsr primary nameserver 94.232.215.2
config dnsr secondary nameserver 0.0.0.0
disable dnsr cache
disable dnsr static

# MLD

config mld ipif System query_interval 125 max_response_time 10 robustness_variable 2
last_listener_query_interval 1 version 2 state disable
config mld ipif 11 query_interval 125 max_response_time 10 robustness_variable 2
last_listener_query_interval 1 version 2 state disable
config mld ipif 12 query_interval 125 max_response_time 10 robustness_variable 2
last_listener_query_interval 1 version 2 state disable
config mld ipif 13 query_interval 125 max_response_time 10 robustness_variable 2
last_listener_query_interval 1 version 2 state disable
config mld ipif 111 query_interval 125 max_response_time 10 robustness_variable 2
last_listener_query_interval 1 version 2 state disable

# DHCP_RELAY

enable dhcp_relay
config dhcp_relay unicast enable
config dhcp_relay hops 4 time 0
config dhcp_relay option_82 state enable
config dhcp_relay option_82 check disable
config dhcp_relay option_82 policy keep
config dhcp_relay option_82 remote_id  default
config dhcp_relay option_82 circuit_id  default
config dhcp_relay option_60 state disable
config dhcp_relay option_61 state disable
config dhcp_relay add ipif svi-1000 100.64.0.10
config dhcp_relay add ipif svi-1001 100.64.0.20
config dhcp_relay add ipif 14 100.64.0.10
config dhcp_relay add ipif 14 100.64.0.20
config dhcp_relay option_60 default mode drop
config dhcp_relay option_61 default drop
config dhcp_relay ports 1-2,5,9,24-25 state disable
config dhcp_relay ports 3-4,6-8,10-23,26-28 state enable

# DHCP_SERVER

config dhcp ping_packets 2
config dhcp ping_timeout 100
disable dhcp_server

# VRRP
```

```
config vrrp ipif System authtype none
config vrrp ipif 114 authtype none
config vrrp ipif 122 authtype none
config vrrp ipif 14_r1 authtype none
config vrrp ipif svi-1000 authtype none
config vrrp ipif svi-1001 authtype none
config vrrp ipif 14 authtype none
config vrrp ipif svi-1001-nat authtype none
disable vrrp

disable vrrp ping

config vrrp trap state disabled

#------------------------------------------------------------------
#            End of configuration file for DGS-3620-28SC
#------------------------------------------------------------------
```