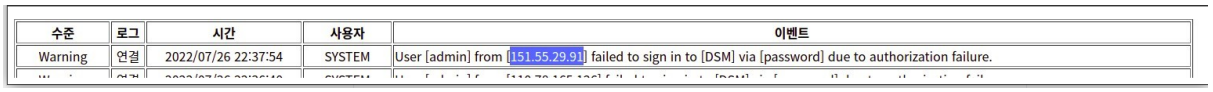
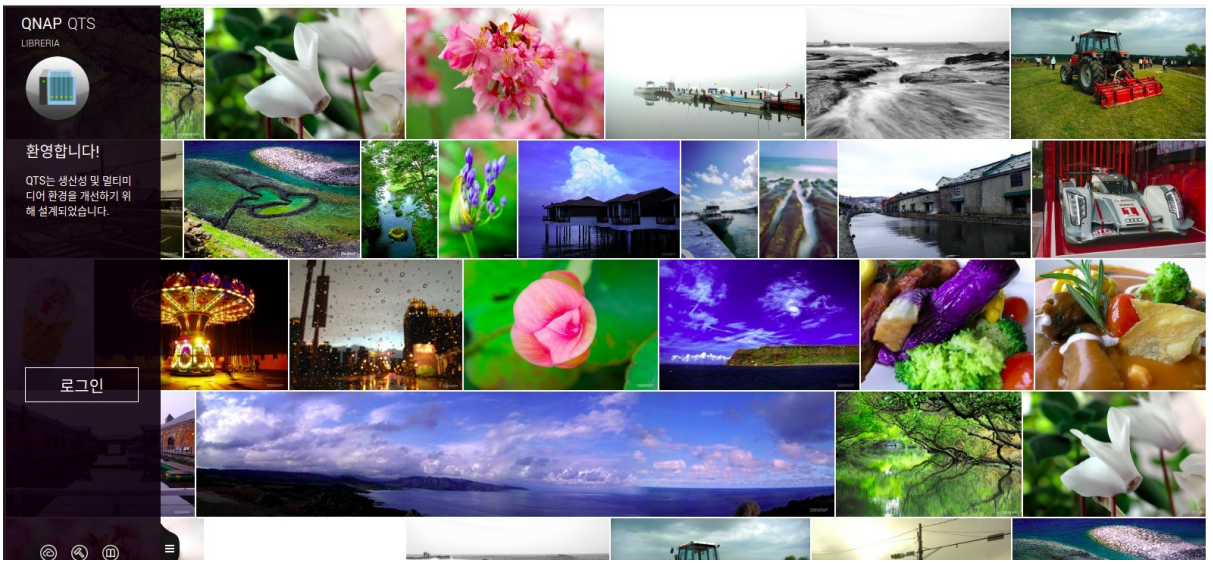
로그인 포털과 역방향 프록시를 이용한 나스의 보안 강화

이번엔 시놀로지 나스의 로그인 포털 과 역방향 프록시를 이용하여 보안을 강력하게 강화 하는 방법에 대한 이야기를 해볼까 합니다.
요즘 많은 사람들이 시노로지 나스등 으로 구축한 클라우드 서버와 웹서버 등등을 이용하려 데이터를 백업 하고 웹서비스를 이용하는 경우가 많은데요
사용자가 급증하면 이를 해킹하여 악용 하려는 악성 트래커 들과 해킹 프로그램 등이 많아지기 마련이죠.

(ex : 시놀로지 나스의 해킹에 이용된 좀비 DSM웹 들)



수준	로그	시간	사용자	이벤트
Warning	연결	2022/07/26 22:37:54	SYSTEM	User [admin] from [151.55.29.91] failed to sign in to [DSM] via [password] due to authorization failure.



수준	로그	시간	사용자	이벤트
Warning	연결	2022/08/03 16:01:45	postfix	User [admin@ kr] from [185.225.73.177] failed to log in via [MailPlus-Server] due to authorization failure.
Warning	연결	2022/08/03 16:01:36	postfix	User [postmaster@ kr] from [185.225.73.177] failed to log in via [MailPlus-Server] due to authorization failure.

최근에 dsm 7. 이전의 dsm 6.대의 업그레이드 가 안된 취약한 운영체제를 중심으로 관리가 안된 나스 시스템을 좀비 서버로 이용 하거나 저장된 데이터 들을 불법 탈취 하려는 시도가 부쩍 많아진듯 합니다.

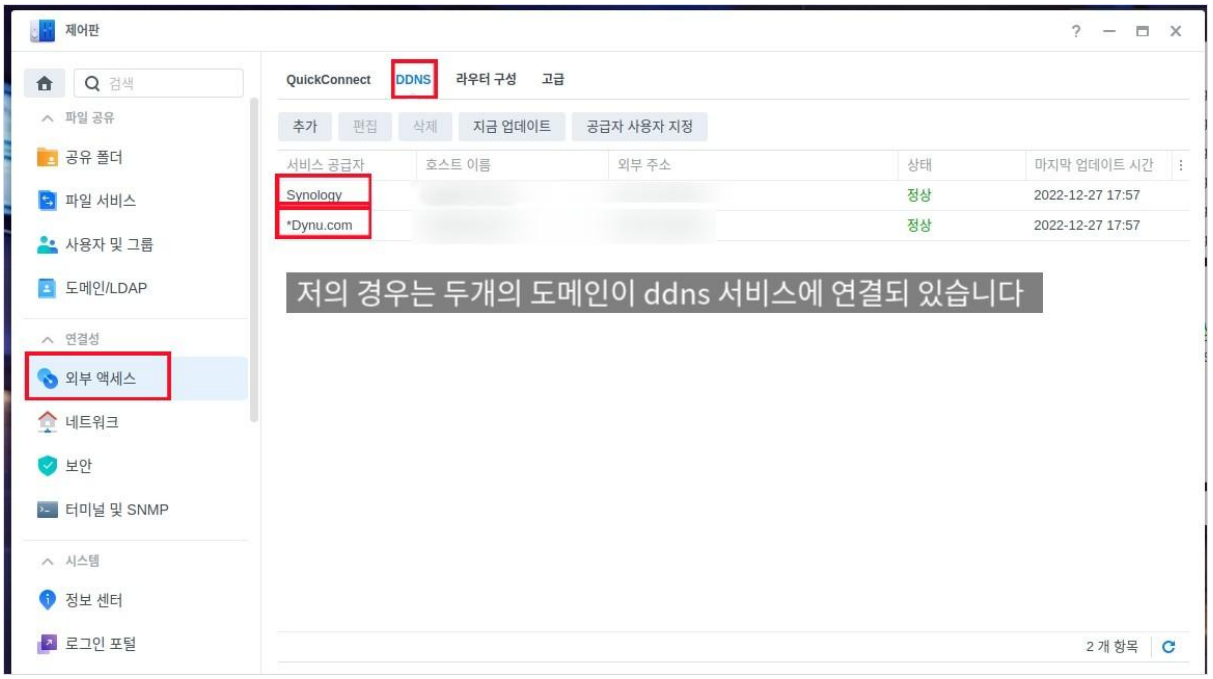
그래서 이번엔 이런 원하지 않는 불청객 들의 무뤠한 침입을 차단할수 있는 시놀로지 나스의 로그인 포털을 이용한 여러 방법들을 설명해 볼까 합니다.

먼저 이를 이용 하기위해서는 시놀로지의 ddns 서비스를 활성화 하고 시놀로지 에서 지원하는 도메인 서비스를 이용해야 합니다만 여기까지 설명 하는것은 스토리가 너무 길어지니 추후에 글을 따로 작성 하기로 하고 이번엔 ddns 서비스 등을 이미 이용하는 사용자 들을 중점으로 리뷰를 작성하려 합니다.

저의 경우는 두개의 도메인이 ddns 서비스에 연결되 있는데요
1.번 시놀로지 나스에서 제공하는 도메인은 로컬내부나 외부 서비스(dsm 과 여러 패키지나 서비스 등을 이용하는 도메인)등 보안이 필요한 서비스에 이용하고 있고.

2.번 Dynu.com 에 DNS 서버를 등록한 DDNS 도메인은 외부에 공개된 개인 블로그나 웹 서비스 등에 이용하고 있습니다.

(DDNS 서비스 이용)

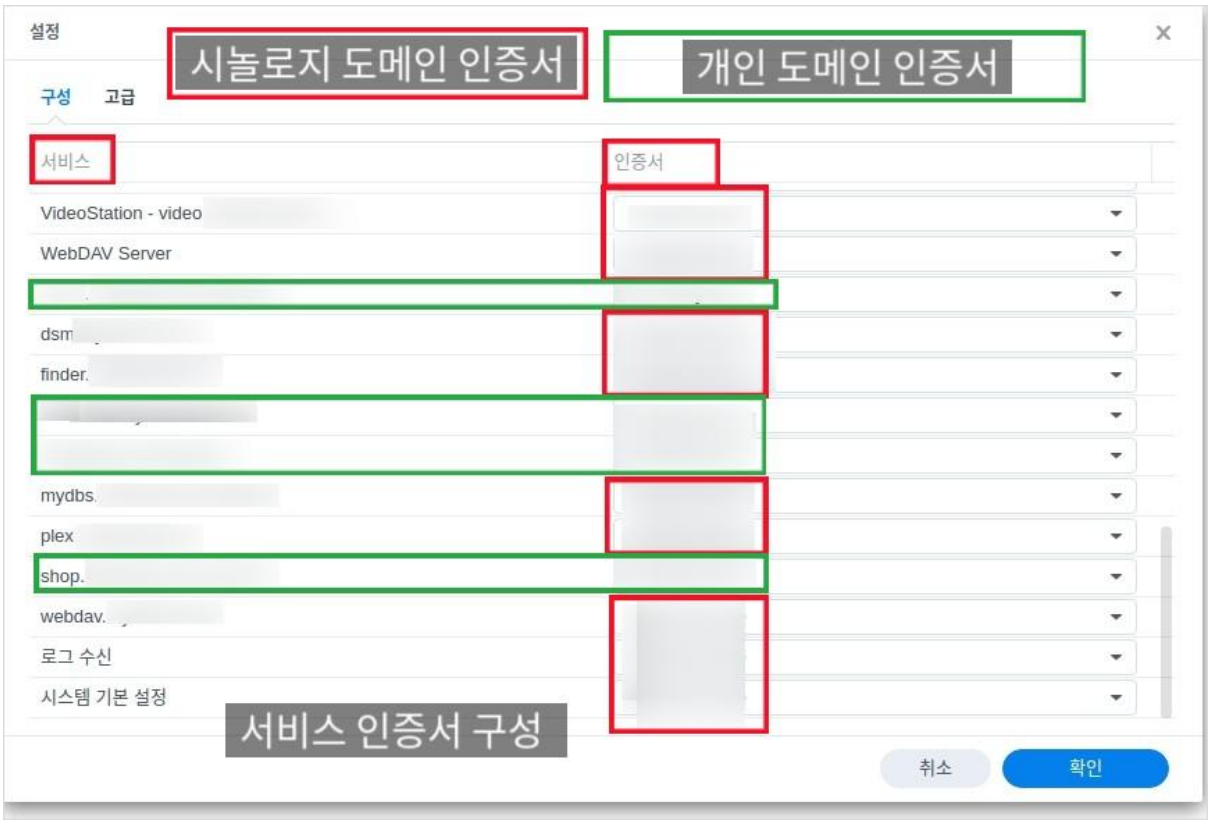


이번 리뷰에 이용된 도메인은 시놀로지 나스에서 제공 하고있는 도메인을 이용한 ddns 서비스 도메인이 중점이 되겠네요.

시놀로지 나스에서 제공 하는 도메인의 경우는 시놀로지 서비스 에서 제공하는 Let's Encrypt 의 인증서를 사용할수 있으며 이를 이용한 서브도메인의 와일드 카드 를 적용할수 있습니다.

(ex : *시놀로지 도메인 인증서)

(ex:서비스에 이용된 인증서 구성)



*시놀로지 로컬 서비스 에는(빨간 선) 시놀로지 도메인의 와일드 카드 인증서로

*웹 서비스 등 외부 서비스 에는 (녹색선) 개인 도메인 으로 구성되 있습니다.

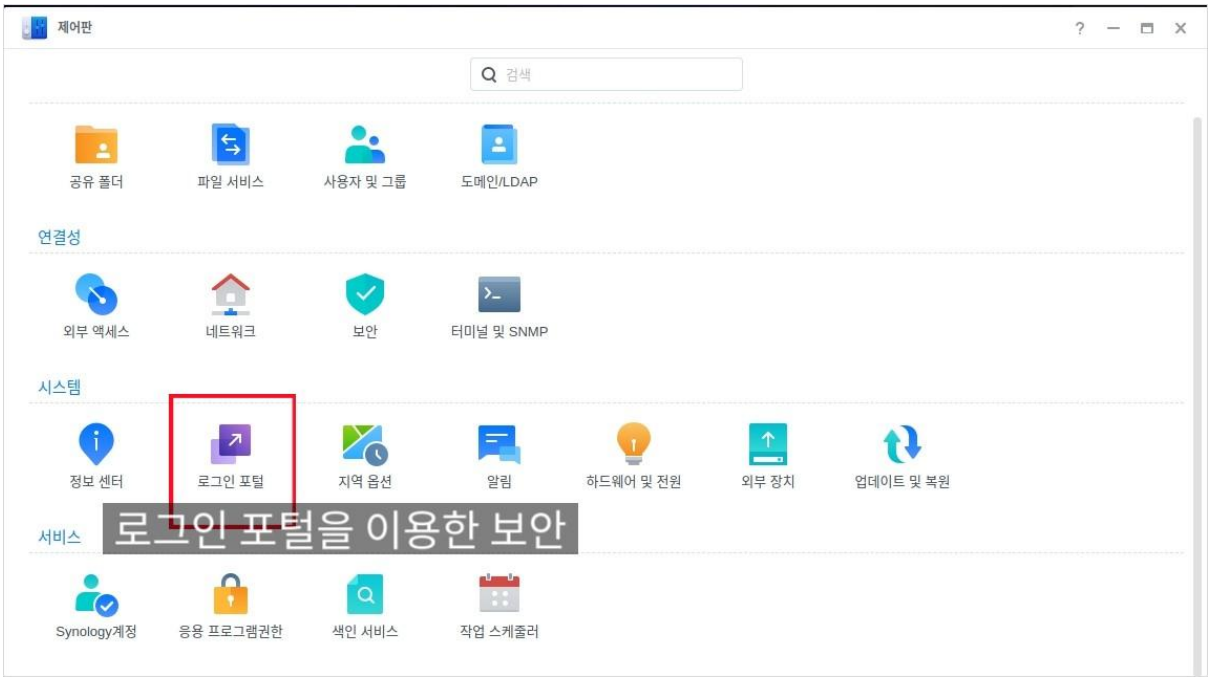
즉 예를들어 각각의 서브 도메인 명.시놀로지 제공 도메인 으로 구성된 와일드 카드로 인증서를 구성 할수 있으니 이를 응용하여 각각의 패키지를 서브 도메인+시놀로지 도메인 으로 구성하여 역방향 프록시로 연결할 예정 입니다.

STEP1. 로그인 포털을 이용한 **DSM** 서비스 도메인 지정

먼저 가장 기본인 시놀로지 운영 시스템인 dsm 서비스를 로그인 포털을 이용하여 시놀로지 도메인 으로 연결해 보도록 하겠습니다.

시놀로지의 **dsm** 버전 **DSM 7.1.1-42962 Update 3** 경우는 로그인 포털의 도메인을 이용한 DSM 설정을 기본으로 로그인 포털 에서 지정할수 있으니 만일 DSN 버전이 DSM 7. 이전인 분들은 보안을 위해서 DSM 버전을 업그레이드 해 주시길 바랍니다.

(*로그인 포털을 이용하여 시놀로지 DSM 서비스를 지정하자)



위에 이미지를 참고삼아 제어판 **->** 로그인 포털 **->DSM** 탭으로 이동하여 간단한 설정 만으로 DSM의 접속을 지정된 도메인 으로 설정 할수가 있습니다.
탭 안의 구성을 보시면 DSN 포트 탭에서 HTTP,HTTPS 포트 설정을 먼저 해주시면 됩니다.

즉 외부 도메인이 호출될 경우 시놀로지 나스의 로컬 서비스인 이 포트로 연결해라 하고 지정해 주는 것이죠.(예 : 5010 / 5011 등등)사용자 들이 DSM 접근 포드를 지정할수 있습니다.

그리고 다음에 도메인 설정 에서 사용자가 지정한 설정한 서브 도메인+ 시놀로지 나스 도메인 을 지정해 주면 되겠죠?(예 : dsm.serves.synology.me 등등)

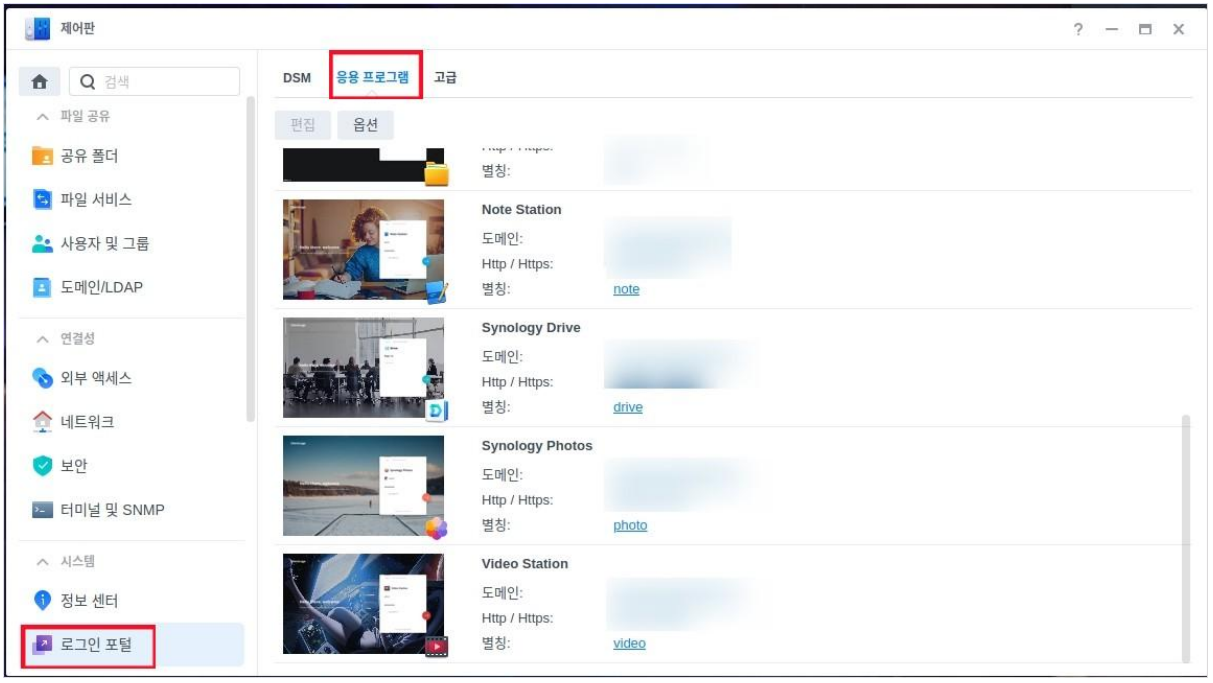
이렇게 도메인과 DSM에 사용될 포트를 지정하여 연결해 놓으면 이렇게 설정된 포트와 지정한 도메인 이 아니면 서비스에 연결이 거부됩니다.(내부 로컬 아이피는 o 외부 접속 불가 X)

이렇게 설정을 하는 주요 논점은 주로 외부에서 침입하는 불청객은 서비스 포트 차원에서 지정된 도메인 으로만 연결되게 해 줌으로 원천적 으로 연결을 거부하는 것이 설정의 중요 포인트 입니다.

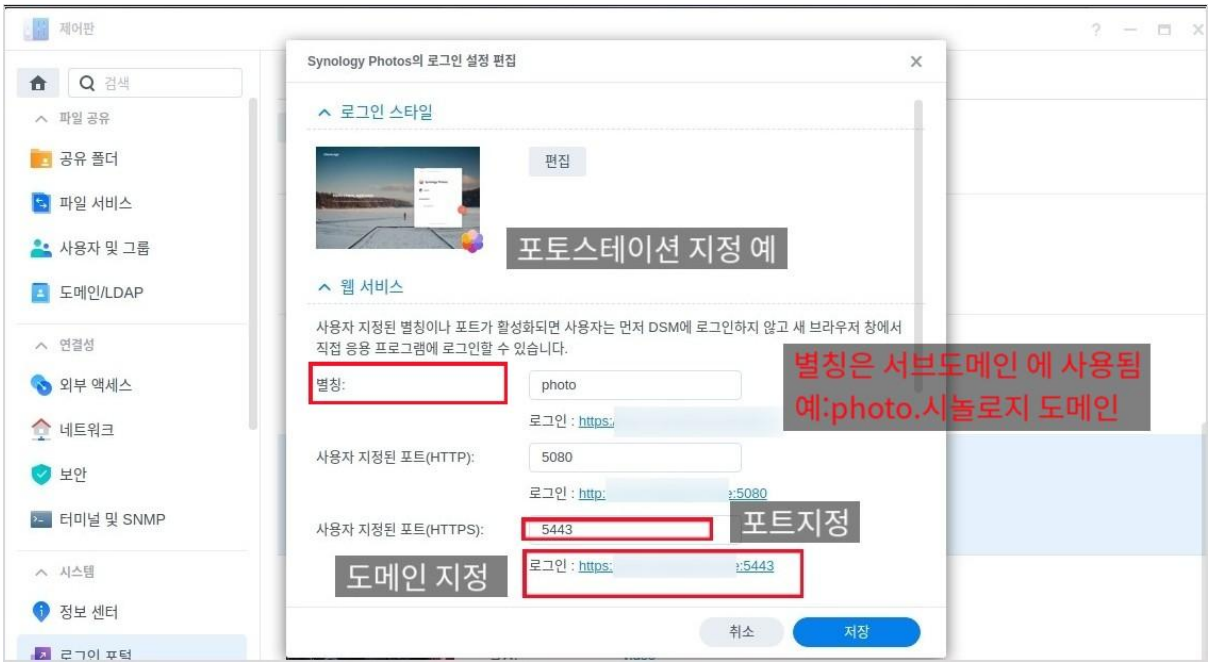
STEP2. 응용 프로그램**(**패키지**)** 들의 도메인 지정

이렇게 가장 기본적인 DSM 시스템 방어를 먼저 해주시고 다음엔 로그인 포털로 넘어 가서 각각의 패키지 들을 또한 비슷한 방법으로 설정해 주시면 됩니다.

(로그인 포털에 이용중인 패키지들)



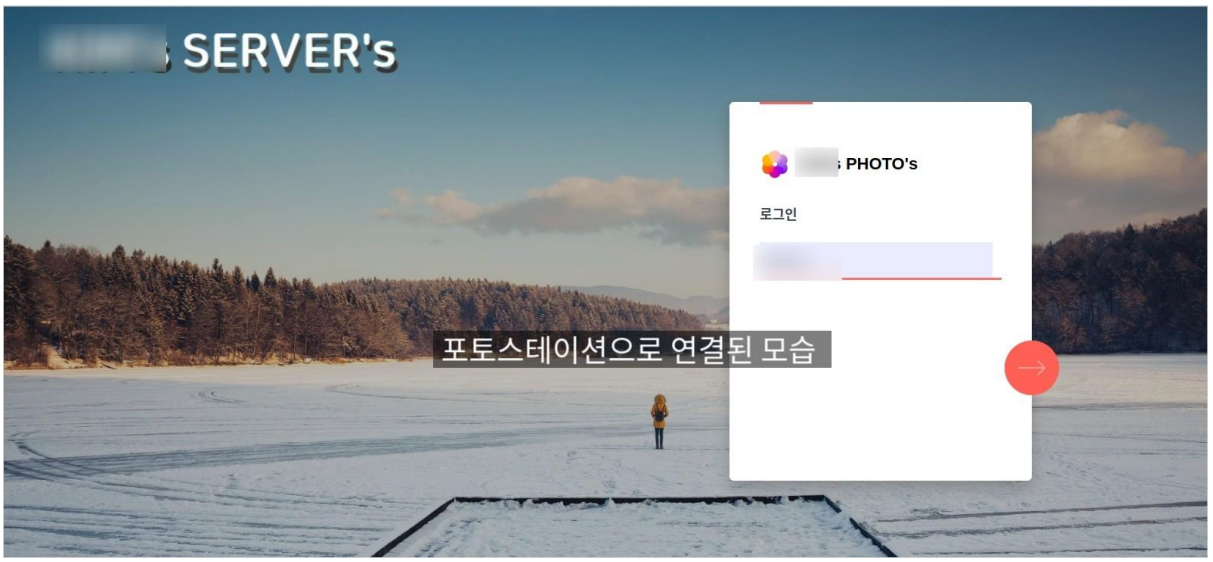
(포토스테이션 패키지의 설정 예)



위에 예를 들어 설정한 포토스테이션 의 패키지의 내용처럼 지정했던 시놀로지 도메인에 앞자리 서브명엔 별칭인 photo 가 들어가며 HTTPS 프로토콜 기준으로 5443 이라는 로컬 포트가 지정 된것을 확인할수 있겠죠?

즉 예 :소스인 photo.시놀로지 도메인으로 서비스 요청이 들어오면 대상 포트인 5443 로컬 포트로 연결하여 포토스테이션 이란 패키지 프로그램을 연결 시켜라 이런 설정과 요청인 것이죠

(*포토 스테이션 연결된 브라우저 창의 모습)



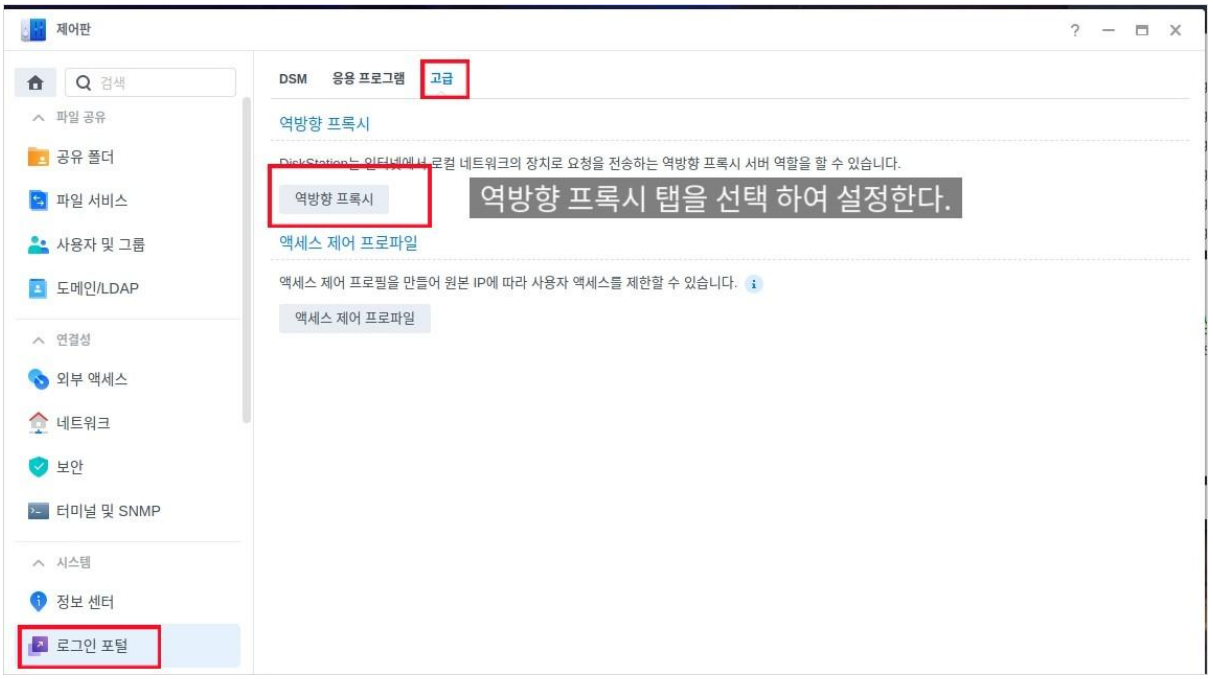
참고 **:** 연결은 pc브라우저나 스마트 폰 등의 앱에서 연결 가능 합니다.
다만 설정에 따라 스마트 폰이나 태블릿의 경우 도메인:80 / 443 의 경우 처럼 기본 웹 포트로 지정해 주어야 스마트 폰 앱 에서 연결해야 연결이 가능한 경우가 있으니 참고 하시기 바랍니다.
이런 식으로 응용하여 시놀로지의 사용 하시는 기본 패키지 들을 웹과 스마트 폰 등의 다양한 디바이스 들에서 프로그램을 자신만 아는 설정된 도메인 으로만 접근할수 있도록 하여서 좀더 보안에 특화된 방법으로 안전하게 사용할수가 있습니다.

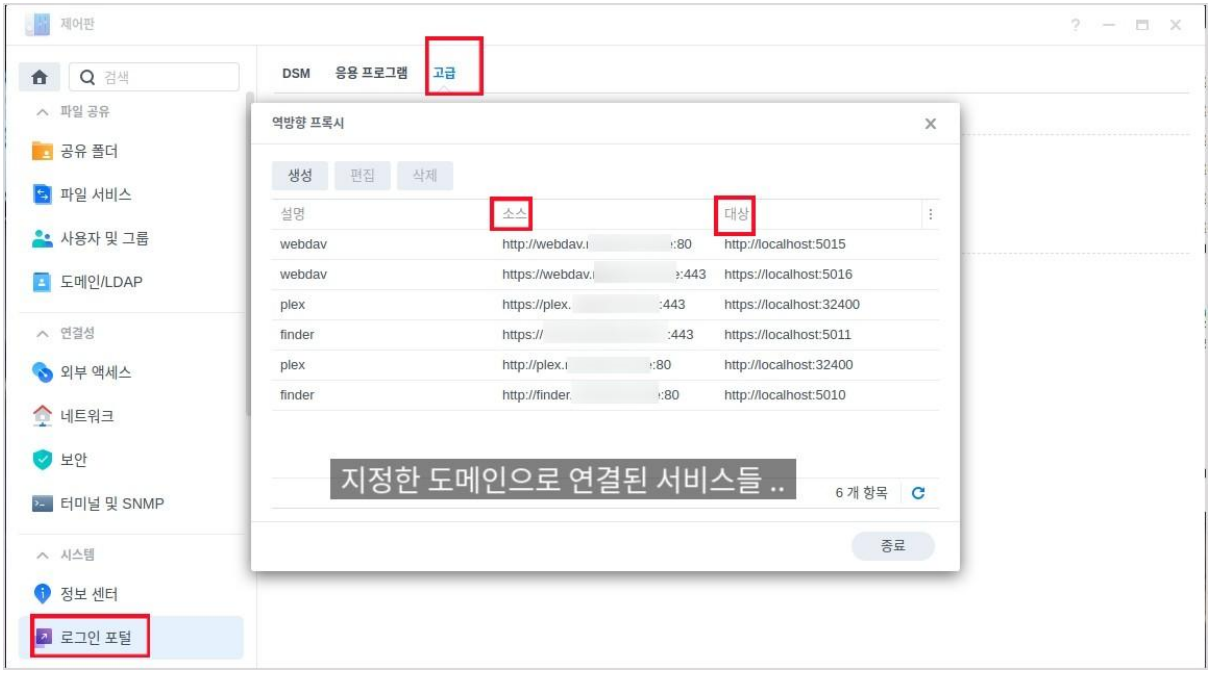
그 외의 시놀로지 기본 패키지로 등록이 안된 서비스 들도 이용할수가 있는데 이때 역방향 프록시를 사용 하시면 됩니다.

STEP3. 그외 서비스 이용방법

이제 패키지로 등록이 안된 서비스 들을 이용하는 방법 입니다
이 설정도 로그인포털 에서 이용할수가 있는데요

로그인 포털에서 고급 -> 역방향 프록시 로 들어 갑니다.





현재 연결된 설정 들을 볼수가 있는데요.
제가 설정한 서비스중 파일 관리를 위한 “WEBDAV “서비스를 예로 들어 보겠습니다.

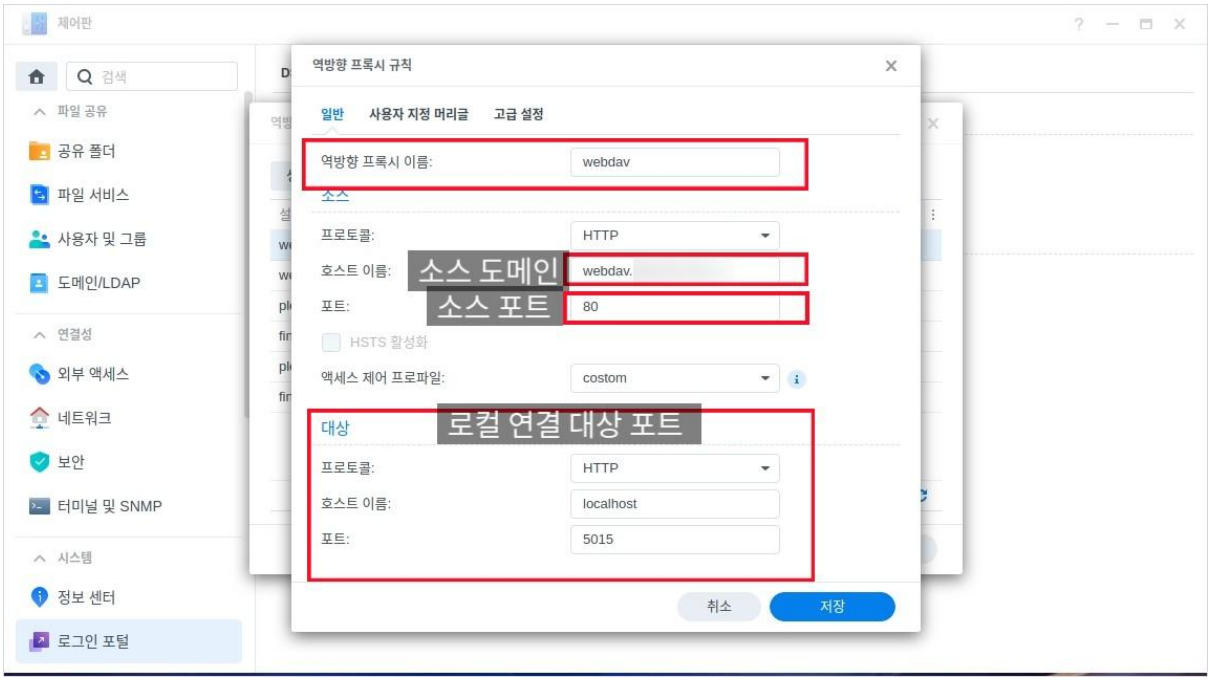
이미지 에서도 직관적으로 보여 지지만 webdav 의 기본 포트인 5015 / 5016 포트가 웹 리소스 포트인 80 / 443 등에서 연결되어 대상포트로 넘어 가는데요

즉 외부 도메인 에서 포트를 지정해 주지 않고 도메인 네임 만으로 (예 : webdav.도메인 네임) 으로 서비스 요청이 들어오면 이를 로컬 서비스인 localhost:5015 / 5016 으로 넘겨주어 webdav 서비스를 이용하는 것이 설정의 요점 입니다.

결국 webdav 서비스를 외부에서 이용할때 지정된 도메인 으로 들어오는 요청만 내부 로컬의 webdav 서비스로 연결이 허락되어 보다 안전하게 서비스를 이용할수 있는거죠

물론 내부망 에서는 로컬 아이피 : 5015 이런 식으로 연결이 가능하며 이외의 외부에 대한 로컬 서비스 로의 접근을 지정한 도메인 접근만 허용하며 근본적으로 막는것이 역방향 프록시의 설정 목표가 되는것 입니다.

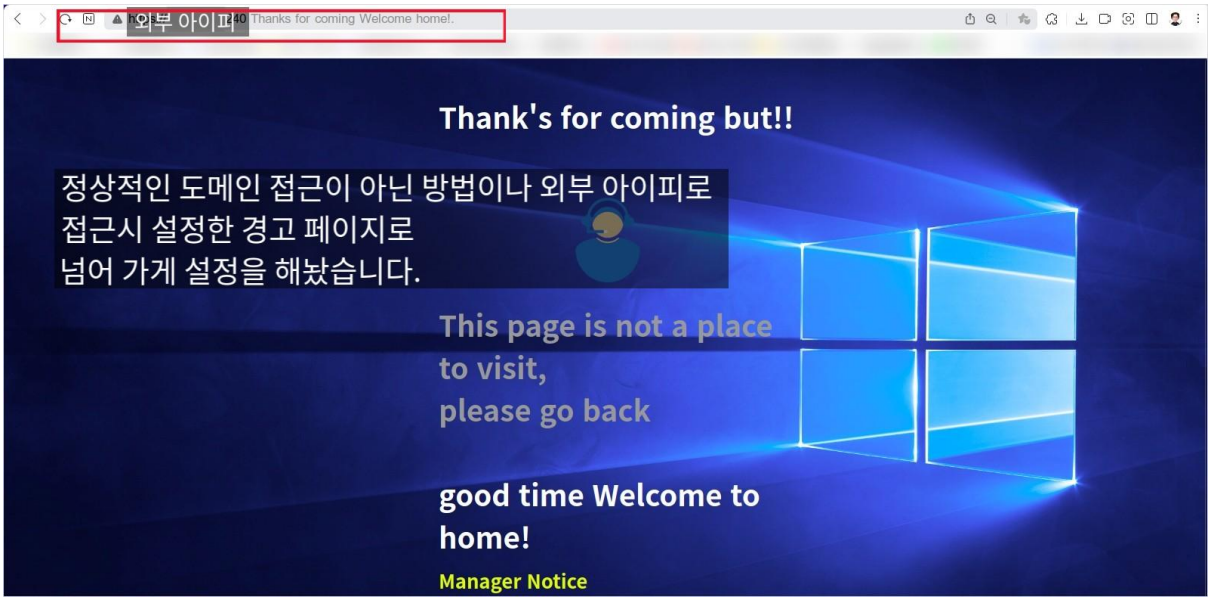
(*역방향 프록시 설정 예)



이런 식으로 이용하면 외부 에서는 서비스에 대한 도메인 을 입력하고 사용자 암호/페스워드 등을 이용하여 접근할수있게 되겠죠.

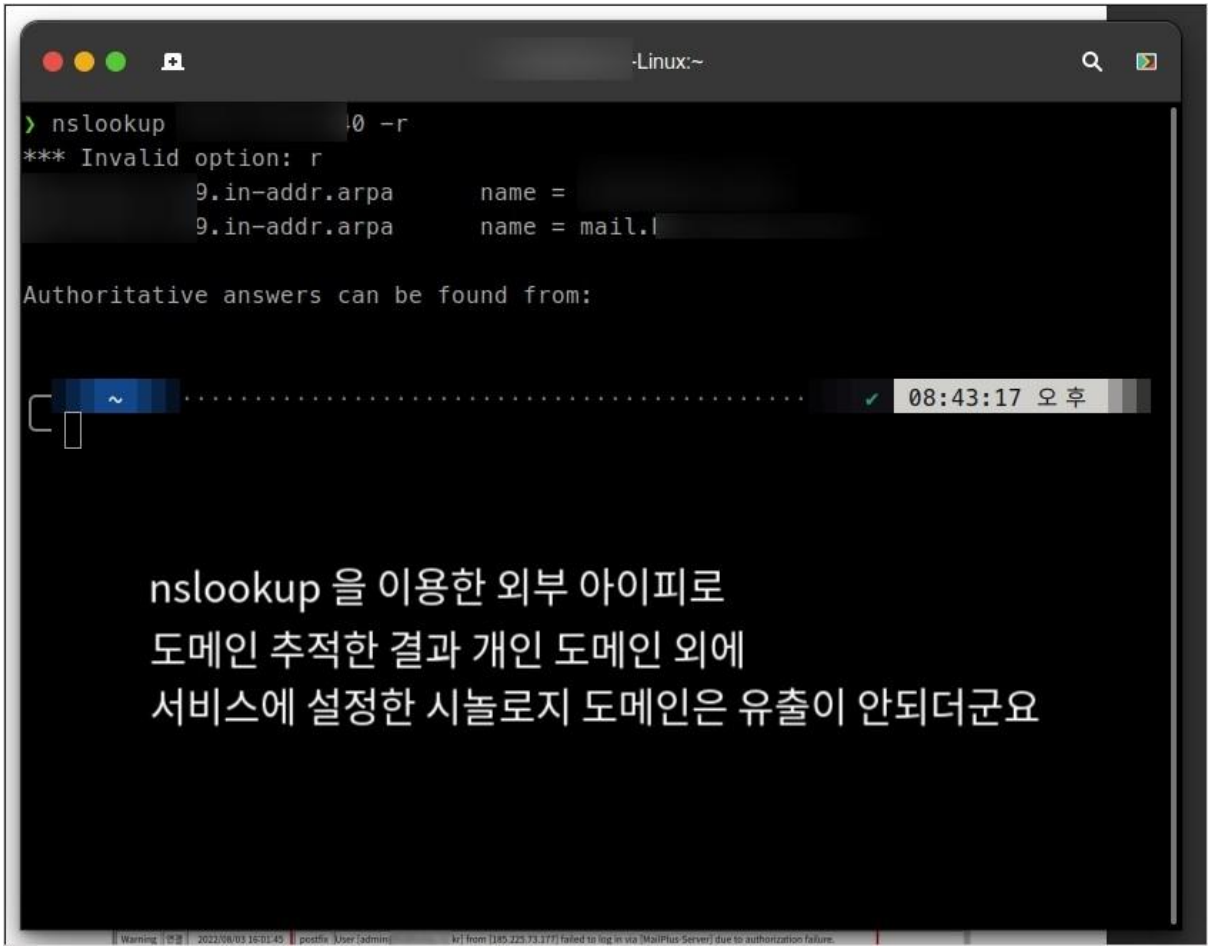
그래서 저같은 경우는 보안이 필요한 패키지나 서비스 들은 유출되지 않는 시놀로지 도메인을 이용하며 그외에 개방이 필요한 서비스 들에게는 외부 공개용 개인 도메인을 이용하여 시놀로지의 보안에 이용하고 있습니다.

예를 들어 지정된 도메인이 아닌 외부 아이피 만으로 접근한 서비스 창을 살펴보죠.



위의 이미지 처럼 지정되지 않은 접근시 위에 보이는 경고 페이지로 연결 되거나 서비스에 연결되지 않는 인터넷 에러가 발생 하도록 설정되어 있습니다.

그리고 nslookup 을 이용하여 외부 아이피로 도메인을 읽어 보았습니다만 외부 DNS 서버를 이용한 외부 도메인 외에 패키지 들에 이용한 시놀로지 도메인은 확인이 안되더군요. 즉 개인이 유출하지 않는 이상 외부에서 시놀로지 패키지 보안에 이용한 서비스는 알수가 없다는 것이 되겠죠?



이처럼 로그인 포털과 역방향 프록시를 이용하여 설정하면 다양한 서비스 들과 패키지 들을 좀더 안전하게 외부에서 이용할수 있습니다.

물론 완전히 개방한 서비스 에 비하여 도메인 유출을 항상 조심해야 하며 설정 하는등의 불편함은 있지만 왜 그런 말이 있죠 불편한 만큼 보안은 안전해 진다는....

저 같은 경우는 이렇게 시놀로지 도메인 서비스를 이용한 역방향 프록시 설정 후 시간당 수십건씩 침입하던 외부 불청객 들이 로그기록 에서 사라지게 되었네요.

요즘 나스등 개인 서버들이 많아지면서 이를 해킹 하여 개인 데이터를 탈취 를 시도하고 심지어 개인 서버들을 좀비화 하여 다른 데이터 서버들을 감염 시키는 해킹 시도들이 많아지고 있는 추세입니다.

조금 더 안전하게 개인 서버를 운영하기 위한 최소한의 방법으로 역방향 프록시 설정에 대한 설명을 이번 글에 리뷰하게 되었습니다.

보안에 100% 완벽한 설정은 있을수 없지만 최소한의 노력으로 자기방어는 해봐야 하지 않을까요?